FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS: PART II

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

JUNE 19, 2013

Serial No. 113–37

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

81–804 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

DARRELL E. ISSA, California, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
PATRICK T. McHENRY, North Carolina
JIM JORDAN, Ohio
JASON CHAFFETZ, Utah
TIM WALBERG, Michigan
JAMES LANKFORD, Oklahoma
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
PATRICK MEEHAN, Pennsylvania
SCOTT DesJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
DOC HASTINGS, Washington
CYNTHIA M. LUMMIS, Wyoming
ROB WOODALL, Georgia
THOMAS MASSIE, Kentucky
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
KERRY L. BENTIVOLIO, Michigan
RON DeSANTIS, Florida

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
JACKIE SPEIER, California
MATTHEW A. CARTWRIGHT, Pennsylvania
MARK POCAN, Wisconsin
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
DANNY K. DAVIS, Illinois
PETER WELCH, Vermont
TONY CARDENAS, California
STEVEN A. HORSFORD, Nevada
MICHELLE LUJAN GRISHAM, New Mexico

Lawrence J. Brady, *Staff Director*
John D. Cuaderes, *Deputy Staff Director*
Stephen Castor, *General Counsel*
Linda A. Good, *Chief Clerk*
David Rapallo, *Minority Staff Director*

Subcommittee on Government Operations

JOHN L. MICA, Florida, *Chairman*

TIM WALBERG, Michigan
MICHAEL R. TURNER, Ohio
JUSTIN AMASH, Michigan
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina

GERALD E. CONNOLLY, Virginia *Ranking Minority Member*
JIM COOPER, Tennessee
MARK POCAN, Wisconsin

CONTENTS

FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS: PART II

Wednesday, June 19, 2013

House of Representatives
Subcommittee on Government Operations,
Committee on Oversight and Government Reform,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:30 a.m., in Room 2154, Rayburn House Office Building, Hon. John Mica [chairman of the subcommittee] presiding.

Present: Representatives Mica, Meadows, Turner, Massie, Issa, and Connolly

Staff Present: Alexia Ardolina, Majority Assistant Clerk; Molly Boyl, Majority Senior Counsel and Parliamentarian; John Cuaderes, Majority Deputy Staff Director; Linda Good, Majority Chief Clerk; Ryan M. Hambleton, Majority Professional Staff Member; Mitchell S. Kominsky, Majority Counsel; Mark D. Marin, Majority Director of Oversight; Laura L. Rush, Majority Deputy Chief Clerk; Scott Schmidt, Majority Deputy Director of Digital Strategy; Peter Warren, Majority Legislative Policy Director; Jaron Bourke, Minority Director of Administration; Adam Koshkin, Minority Research Assistant; Safiya Simmons, Minority Press Secretary; and Cecelia Thomas, Minority Counsel.

Mr. Mica. Good morning. I would like to call this hearing to order and welcome everyone to the Subcommittee on Government Operations. Mr. Connolly and I appreciate your being with us.

The topic of today's subcommittee hearing is Federal Government Approaches to Issuing Biometric IDs, and this is actually the second part. We had hoped to get everybody on one panel and we discussed primarily the TWIC card and its shortcomings at the last hearing. This hearing focuses on some of the other Federal agencies that are producing identification and credentialing, primarily for Federal workers and others in transportation and others who seek access to what should be secure areas or facilities.

So, with that being said on our topic today, welcome our witnesses. We will hear from you in a minute. We will start today's proceedings and the order of business will be, first, opening statements by myself and Mr. Connolly and any other members that join us. I see Mr. Massie has joined us too. Our subcommittee will then hear from the witnesses. We will hear from all the witnesses and then we will take some time to do questions. We will wait until we have heard from all of the witnesses to do that.

We have an important mission statement. I won't read the whole thing today, but we have a responsibility to ensure that the obligations to taxpayers are met; that we carefully review the performance of various Government programs. You have authorizers and you have appropriators, and they have their mission. Early on in our Government they created this committee and its predecessor to review how agencies and Government entities were following through with both the intent of the law and then the manner in which funds have been appropriated, and that is the purpose of the Government Oversight and Reform Committee, general purpose.

Again, today, having been involved in this whole process since 9/11, the good Lord somehow put me in charge of aviation back in 2001, early in the year, and little did we know what would happen with 9/11 and all the aftermath of 9/11. I had the obligation and responsibility to put together some programs and try to make certain that we put in place mechanisms for the best security possible.

One of the things that we looked at was credentialing and, of course, when we started back in 2001, after creating TSA and looking at some of the other needs, try to make certain that we had exact identifications of those who were involved in transportation and accessing secure facilities. We immediately saw the need for some standards and it was back in 2004 that President Bush actually issued a directive and set some standards, and those are still in place today, it was Homeland Security Presidential Directive 12, and the issuance of that set standards that are supposed to prevail today. Unfortunately, many agencies have not made significant progress in implementing the biometric standards.

We are going to hear from the agency that actually sets those standards. I am very concerned that time and time again, and in previous hearings, I have been promised that the standards are just about to be set, just going to be a matter of months. In fact, maybe the staff can get me the last commentary.

Now I am told that the last person that testified and told me that it was just a matter of months before those standards are set is now retiring from the Federal workforce, so probably the first question I will have for her replacement is when do you plan to retire. But, again, without those standards being set, sometimes the agencies who are testifying before us are left in the lurch without a standard set by the Federal Government.

A dual biometric measure is something we have always sought after, and that is in the form of both fingerprints and also iris. If you have those two biometric measures, you can almost guarantee that the person with the credentialing is that person.

We will hear also from, I believe, one of the witnesses about the ability to abuse credentialing and some of the problems even with using fingerprints as a sole source of identity.

We looked at the TWIC program, and let me run through some of the programs that we have pretty quickly. I think Mr. Connolly may recall some of the testimony. We spent over half a billion dollars on a TWIC card. We have issued more than 2 million of them. Now we are reissuing some of them. The TWIC card does not have full biometric dual capability; it has some fingerprint capability. Unfortunately, it also does not have a reader.

And most recently we got a request to maybe do away with a requirement for readers. So we spent half a billion dollars on a pretty expensive ID program that could have been done at a fraction of the cost. It almost defies reason that we could go this long, not produce a card that could be used, and still don't have a biometric standard or incorporation of that capability in the TWIC card, and we are on our second set of issuing these expensive I call them college IDs, as any college kid could produce probably the same thing off of his computer.

We have gone around and around with the FAA on a pilot's license. Some of you may recall that in the past, in fact, in law, we set a pilot's license, which used to be a little folded piece of paper, we set in law that it had to be durable, it had to have a biometric capability, and it had to have a photo of the pilot on it.

Lo and behold, several years ago a pilot approached me and said, have you seen the new pilot's license? Where is the new pilot's license? And the pilot's license was durable. I have one of these here. It was durable. The strip was not really biometric capable. In fact, anything in your wallet, any credit card would have better capability than the biometric capability of the card.

You see the front of the card up there; I have the back of the card. The only pilot photo on the card were Wilbur and Orville Wright. This is not a joke; this is what we have for a pilot's license. So we still don't have a credential for a pilot, a commercial pilot. This is what we have.

Now, last week, when we did our hearing out in Dayton, you weren't there, I actually had a chance to go to the Wright graveyard.

Mr. CONNOLLY. Believe me, I wanted to be in Dayton.

Mr. MICA. Yes. Well, I went to the Wilbur and Orville Wright graveyard. Their tombs are here. Both of these pilots are dead; I can confirm it. I have been to the site, quite interesting, if you ever get out to Dayton. It is in Mr. Turner's, who is a member of our committee, his district. But the only pilots on this license produced to this date are Wilbur and Orville Wright, certifiably dead.

So that is the pilot's license. And when you talk to FAA, they say, well, DHS has to set the standards and TSA, and then they point to, again, the National Standards Bureau, who hasn't set a standard. And, again, that lady is retiring, so we will talk about that in a few minutes.

We have 924,000 airport workers, all who have various forms of credentialing; none of it standard, none of it, again, with full biometric capability, maybe one or two of them may have incorporated. We don't even know. TSA has started a pre-check program and I have had an experience with that personally. I was able to get on, my wife was not able to get on.

I don't want to complain about that, but I guess it is based on the number of miles that you have. I understand they have a precheck lite, which is going to be interesting, so you don't have to have quite as many miles. But even if you have that capability, and it is encoded in your boarding pass, you still do not have any credentialing, and you don't know for certain who the person is who has the pre-checked clearance. I could thwart the pre-check in a nanosecond, and anyone who is intent on imposing a terrorist act could do the same.

Then, again, our own personal experience, and I have to relay this to the committee, is my wife couldn't get in pre-check, so they said go Global Entry. So after waiting a long time and paying the fee, which we did, she finally got her Global Entry. There are 734,000 people she has joined with Global Entry.

And she got her card and proudly displayed it, but found out that the form to apply was not properly crafted to get the information needed, so her middle name, which is Evelyn, is on her Global card, but it doesn't match her passport, which has her maiden name. So, again, she has a card with fingerprints, with no iris, and you have conflicting documents.

Of course, the passport, and I remember beating years ago with the passport folks, trying to get them onboard to have dual identity. They produced that without that capability. So we have millions of passports issued, again, without dual biometric capability.

We also have NEXUS with 850,000 people; no bio. We have FAST; I guess it is a trucker and cargo program; 80,000, no bio. We have dual bio. We have three quarters of a billion air travelers to go through with various documents, driver's license and any kind of public ID, most of which, again, can be easily forged and used in an improper manner.

There is a little bit of good news. The private sector has produced a CLEAR card. Do we have a CLEAR card? This actually has a biometric. Now, it doesn't have a standard. I guess TSA or somebody must have checked off on a CLEAR card, but it is not the standard set by the Federal Government or a standards agency, but it has a dual biometric capability.

One of our subcommittees visited, a year or so ago, Canada, and since 2007 they have had, it is called RAIC, Restricted Area ID Card, and all of their airports and airport workers, personnel across Canada, 28 airports, about one-tenth of what we have in size, but they all have dual biometric credentialing and it also has different standards for entry and clearance; and they have had that in place since 2007.

So that is a little bit of background. We have spent billions of dollars on these credentialing. I think we have left ourselves at risk. We don't know who is coming and going, whether it is passengers, airport workers, transportation workers, pilots. But we have spent an incredible amount of money and it is absolutely mind-boggling that we do not have, at this stage, proper credentialing or anything that even comes close to complying with the intent of Congress or some of the standards that were set back in 2004.

So a little bit of a long introduction, but some of the information and background that I wanted to cover this morning.

Mr. Connolly?

Mr. CONNOLLY. Thank you, Mr. Chairman, and thank you for your passion on this subject, which is quite evident, and it is important.

You referenced our first hearing on this subject and I remember it quite visibly, and this is a topic that demands much more attention. At our previous hearing we talked about the failure of the TWIC program and we talked about programs that worked. The chairman just cited the CLEAR card in the private sector, but in Afghanistan and Iraq millions of contractors and civilian personnel have been issued ID cards that work; very few of the incidents of people being able to misuse those cards and breach security.

If we can do it in the theater of war, why can we not replicate that, or at least the best elements of that, here at home? And the failure to do so is an ongoing source of distress, I hope for you and certainly for us up here.

So I really want to have a dialogue this morning, Mr. Chairman, about what can we do to ramp this up and make it efficacious. Something that doesn't violate people's privacy or civil liberties but, on the other hand, protects the Country and is more efficient than the current systems we have of screening mass members of citizens and transport modes throughout the Country, including airports.

So I am looking forward to your testimony and I very much want to hear ideas. I will say, parenthetically, the chairman noted that we had a witness who made assurances about deadlines being met and things happening. She had to know she was retiring. She had to know that she wouldn't be accountable after that hearing.

And that is disappointing because this is about the Nation's security and we are all actually on the same team trying to get at what works and what doesn't, and, frankly, that kind of behavior is most disappointing, if not disingenuous, and I would hope it would be avoided in the future.

Anyway, with that, I look forward to the testimony this morning and working with our colleagues in the executive branch to try to resolve this issue for the sake of security of the Country.

Thank you, Mr. Chairman.

Mr. MICA. Thank you, Mr. Connolly.

All members may have seven days to submit opening statements for the record.

Now we will go to our first panel. I guess we have two panels today. Oh, it is all one? Okay. You are the first and only.

Mr. Charles Romine is the Director of Information Technology Laboratory with the National Institute of Standards and Technology; Mr. Steven Martinez is the Executive Director of the Science and Technology Branch with the Federal Bureau of Investigation; Mr. John Allen is the Director of the Flight Standards Service with the Federal Aviation Administration; Ms. Colleen Manaher is Executive Director of Planning, Program Analysis, and Evaluation with Customs and Border Patrol; we have Ms. Brenda Sprague as the Deputy Assistant Secretary for Passport Services in the Department of State.

Now, part of this committee's work, or most of this committee's work is investigative. We do, as part of our procedure, swear in our witnesses, so the first thing we are going to do is ask you to stand, raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give before this subcommittee of Congress is the whole truth and nothing but the truth?

[Witnesses respond in the affirmative.]

Mr. MICA. All of the witnesses answered, the record will reflect, in the affirmative.

Well, welcome today. We are going to start with Mr. Charles Romine, Director of Information Technology Laboratory at the National Institute of Standards and Technology.

Mr. Connolly, Mr. Romine is the replacement for Ms. Cita Furlani, and she testified before the House Transportation and Infrastructure Committee on April 14th, 2011, but by the end of that year, in fact, there is a question here, it says by the end of the year she would have the standards available, and she said, oh, yes, yes. Now, I guess I can't hold her in contempt since she is retired, but we have Mr. Romine here today to update the committee on not only this time was I told that these standards were right around the corner, but several other times, and we can document that.

This will be made part of the record. Without objection, so ordered.

Mr. MICA. So we will hear from you first, sir. Welcome and you are recognized.

STATEMENT OF CHARLES H. ROMINE

Mr. ROMINE. Chairman Mica, Ranking Member Connolly, and members of the subcommittee, I am Chuck Romine, Director of the Information Technology Laboratory at NIST. Thank you for the opportunity to appear before you today to discuss the NIST role in standards and testing for biometrics.

NIST has nearly five decades of experience in proving human identification systems. NIST responds to government and market requirements for biometric standards by collaborating with Federal agencies, academia, and industry to support development of biometric standards, conformance testing architectures and tools, research advanced biometric technologies, and develop metrics for standards and interoperability of electronic identities.

NIST research provides state-of-the-art technology benchmarks and guidance to U.S. Government and industries. To achieve this, NIST actively participates in Federal biometric committees and national and international standards developing organizations.

Biometric technologies can provide a means for recognizing individuals based on one or more physical or behavioral characteristics. These can be used to establish or verify personal identity of enrolled individuals. By statute and administrative policy, NIST encourages and coordinates Federal agency use of voluntary consensus standards and participation in the development of relevant standards, and promotes coordination between the public and private sectors in the development of standards and conformity assessment activities.

NIST collaborates with industry to develop a consensus standard that is used around the world to facilitate interoperable biometric data exchange. The standard is evolving to support law enforcement, homeland security, forensics, and disaster victim identification.

Internationally, NIST leads development of biometric standards that have received widespread market acceptance. Use of these standards is mandatory by large international organizations for identification and verification of travelers at border crossings.

In response to Homeland Security Presidential Directive 12, NIST developed a standard to improve the identification and authentication of Federal employees and contractors for access to Federal facilities and IT systems. NIST is updating the standard and guidelines to include optional use of iris images for biometric authentication; use of facial images for issuance, re-issuance, and verification processes; and privacy-enhancing on-card comparison.

NIST leads the development of conformance tests for implementations of national and international biometric standards. In August of 2010, NIST released conformance tests designed to test implementations of finger image and finger minutiae biometric data interchange format specified in four American national standards, and in 2011 we released conformance tests designed to test implementations of the international iris image data interchange format standard.

Understanding capabilities and improving performance of biometric technologies requires a robust testing infrastructure. For more than a decade, NIST has been conducting large biometric technology challenge programs to motivate the global biometric community to dramatically improve the performance and interoperability of biometric systems, foster standards of option and support global deployment, and achieve an order of magnitude that are accuracy gains.

One example is the Iris Exchange, or IREX, testing program initiated at NIST in support of an expanded marketplace of iris-based applications based on standardized interoperable iris imagery. The work is conducted in support of the ISO and ANSI/NIST standards. The IREX III testing program evaluated large-scale one-to-many iris identification algorithms.

The NSTC National Biometrics Challenge 2011 report included key challenges to the future applications of biometrics technologies, including research in the privacy and usability of biometrics. For privacy, NIST is collaborating to advance technical methods to safeguard and control the use of biometrics through methods such as liveness detection and biometric template protection.

Usability is a priority for deploying biometric systems within the Federal Government. NIST was identified in a recent National Academies report as one of only two organizations addressing usability in biometric systems. NIST has applied its usability expertise to several studies involving biometric systems. As a result of one study, all of the fingerprint standards at U.S. ports of entry are now angled to improve the collection process.

In summary, NIST has a diverse portfolio of activities supporting our Nation’s biometric needs. With NISTs extensive experience and broad array of expertise, both in its laboratories and in collaboration with U.S. industry and with other Government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable biometric systems.

Thank you for the opportunity to testify on NISTs activities in biometrics, and I would be happy to answer any questions that you may have.

[Prepared statement of Mr. Romine follows:]

Testimony of

Charles H. Romine
Director
Information Technology Laboratory
National Institute of Standards and Technology
United States Department of Commerce

Before the

Subcommittee on Government Operations
Committee on Oversight and Government Reform
United States House of Representatives

"Standards for Biometric Technologies"

June 19, 2013

Chairman Mica, Ranking Member Connolly and Members of the Subcommittee, I am Chuck Romine, Director of the Information Technology Laboratory (ITL) at the Department of Commerce's National Institute of Standards and Technology (NIST). Thank you for the opportunity to appear before you today to discuss our role in standards and testing for biometrics and identity management as it relates to the incorporation of biometric technologies into agencies identification card programs.

The Commerce Department's mission is to help make American businesses more innovative at home and more competitive abroad. The development of technically sound measurements, testing and standards are essential for the successful deployment of technologies upon which our society depends. NIST, a non-regulatory agency within the Department works specifically to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST accelerates the development and deployment of information and communication systems that are interoperable, secure, reliable, and usable; advances measurement science through innovations in mathematics, statistics, and computer science; and develops the measurements, testing, and standards infrastructure for emerging information technologies and applications.

NIST has nearly five decades of experience improving human identification systems. NIST responds to government and market requirements for biometric standards by collaborating with other federal agencies, academia, and industry partners to:

- Support the timely development of biometric standards.
- Develop the required conformance testing architectures and testing tools to test implementations of selected biometric standards.
- Research measurement, evaluation and standards to develop and advance the use of biometric technologies including fingerprint, face, iris, voice, multi-modal techniques, and emerging identity determination technologies from video.
- Develop common models and metrics for identity management, critical standards, and interoperability of electronic identities.

These efforts improve the quality, usability, interoperability and consistency of identity management systems, protect privacy, and assure that U.S. interests are represented in the international arena. In fact, NIST research has provided state of the art technology benchmarks and guidance to U.S. Industry and U.S. Government, who depend upon biometrics recognition.

To achieve this impact, NIST actively participates in the National Science and Technology Council (NSTC) Subcommittee on Biometrics and Identity Management and its Standards and Conformity Assessment and Research, Development, Test, and Evaluation Working Groups as well in several USG interagency biometric working groups.

In addition, under the provisions of the National Technology Transfer and Advancement Act (PL 104-113) and OMB Circular A-119, NIST is tasked with the role of encouraging and coordinating federal agency use of voluntary consensus standards and participation in the development of relevant standards, as well as promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities. NIST works with a wide variety of standards and specification developing organizations, which have vastly different models by which they develop their technical standards and specifications, but all of which are also characterized by active industry participation. NIST has about 400 NIST staff participating in approximately 120 standards and specification developing organizations. NIST leads national and international consensus standards activities in cryptography, biometrics, electronic credentialing, secure network protocols, software and systems reliability, and security conformance testing – all essential to accelerate the development and deployment of information and communication systems that are interoperable, reliable, secure and usable.

BIOMETRIC TECHNOLOGY

Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to establish or verify personal identity of individuals previously enrolled. Examples of physical characteristics include face photos, fingerprints, and iris images. An example of behavioral characteristic is an individual's signature. Used with other authentication technologies, such as tokens, biometric technologies can provide higher degrees of security than other technologies employed alone. For decades, biometric technologies were used primarily in law enforcement applications, and they are still a key component of these important applications. Over the past several years, the marketplace for biometrics solutions has widened significantly and today includes public and private sector applications worldwide.

NIST'S BIOMETRIC STANDARDS ACTIVITIES

Voluntary Consensus Standards
Most Standards Developing Organizations (SDOs) are industry-led private sector organizations. Many voluntary consensus standards from those SDOs are appropriate or adaptable for the Government's purposes. According to OMB Circular A119, the use of such standards by U.S. Government Agencies, whenever practicable and appropriate, is intended to achieve the following goals:

- Eliminate the cost to the Government of developing its own standards and decrease the cost of goods procured and the burden of complying with agency regulation.
- Provide incentives and opportunities to establish standards that serve national needs.
- Encourage long-term growth for U.S. enterprises and promote efficiency and economic competition through harmonization of standards.
- Further the policy of reliance upon the private sector to supply Government needs for goods and services.

When properly conducted, standards development can increase productivity and efficiency in Government and industry, expand opportunities for international trade, conserve resources, improve health and safety, and protect the environment.

NIST Information Technology Laboratory (ITL) – An American National Standards Institute (ANSI)-accredited SDO

Under our 1984 accreditation by ANSI, the private-sector U.S. standards federation, NIST continues to develop consensus biometric data interchange standards. Starting in 1986, NIST has developed and approved a succession of data format standards for the interchange of biometric data. The current version of this standard is ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*. This standard continues to evolve to support Government applications including law enforcement, homeland security, as well as other identity management applications. This standard, used around the world, facilitates interoperable biometric data exchange across jurisdictional lines and between dissimilar systems developed by different manufacturers. In addition to the exchange of fingerprint, latent, face, and iris biometric data, the 2011 version of the standard includes new modalities (DNA and plantar) as well as a latent print extended feature set (EFS); forensic image markups for face and iris; images of all body parts, new metadata fields such as geoposition of sample collection; biometric data hashing and information assurance; and data handling logs.

NIST researchers are collaborating with biometrics and forensics experts worldwide to further expand the ANSI/NIST-ITL Standard to support forensics and Disaster Victim Identification (DVI). Currently an update is underway to include the introduction of dental data, pattern injury (e.g., bite marks) data, and forensics and investigatory voice data. The update will include new capabilities, such as x-rays and other medical imaging technologies. The additions will promote U.S. and international interoperability for forensics data pertaining to identity, and establish for the first time the exchange of dental information among various systems (such as that used by the Federal Bureau of Investigation (FBI) and INTERPOL and the ones used by medical examiners). NIST has also worked with the biometrics and forensics community to introduce within the ANSI/NIST-ITL Standard a new extended feature set to support the interoperable exchange of latent print feature data between human examiners and with automated fingerprint identification systems (AFIS).

ISO/IEC Joint Technical Committee 1, Subcommittee 37- Biometrics

From the inception of JTC 1/SC 37 in 2002, NIST has led and provided NIST experts to develop international biometric standards in this SDO. JTC 1/SC 37 developed standards have received widespread international and national market acceptance. Large international organizations, such as the International Civil Aviation Organization (ICAO) for Machine Readable Travel Documents (MRTD) and the International Labour Office (ILO) of the United Nations for the verification and identification of seafarers, specify in their requirements the use of some of the international biometric standards developed by JTC 1/SC 37.

The ICAO has moved the world's passports to a new level of travel document security, data integrity and identity management. To facilitate the goal of global interoperability, ICAO selected facial recognition as the globally interoperable biometric (listed as mandatory) for machine-assisted identity confirmation for MRTD. Additionally, ICAO selected, as options, the ability to incorporate the specifications for finger and iris. The ICAO estimate as of December 2012 was that there were 430 million ePassports existing, issued by 108 countries using the JTC 1/SC 37 standards for this application. This program serves as a model for effective collaboration and cooperation between industry through Subcommittees of ISO/IEC JTC 1 and the governments of the world through ICAO. ILO's requirements included the first edition of the finger minutiae and finger image data interchange formats developed by JTC 1/SC 37.

Representative examples of applications in different countries referring to biometric international standards include Spain (for their electronic national identity card and the Spanish e-Passports),, and India (which is deploying one of the world's largest identity assurance systems relying on standards-based biometrics technologies).

Biometric Standard for Mobile Applications

Federal agencies require that their biometric results exchange information with emerging mobile applications, making operations more effective and efficient while improving relevant information sharing associated with a biometric. NIST researchers, with support from DHS and the FBI's Biometric Center of Excellence, developed a protocol for communicating with biometric sensors over wired and wireless networks—using web technologies. The new protocol, called WS-Biometric Devices, allows desktops, laptops, tablets and smartphones to access sensors that capture biometric data such as fingerprints, iris images and face images using web services. The WS-Biometric Devices protocol enables interoperability by adding a device-independent web-services layer in the communication protocol between biometric devices and systems. This work is being developed by a private sector SDO. NIST also is working with industry through the Small Business Innovation Research Program to help bring these plug-and-play biometric devices to market.

Mobile applications typically require a rapid response over limited bandwidth communication channels. To meet performance requirements, so-called "lossy compression" must be applied, but as the name implies, data information is lost as the compression is performed, and this data loss can impact system accuracy as well as interoperability. NIST research measures and analyzes the effects of varying amounts of lossy compression and NIST is working with the biometrics community to establish biometric data transmission profiles that employ well-informed compression best practices.

Homeland Security Presidential Directive (HSPD)-12/ FIPS 201

In response to HSPD-12 (August, 2004), NIST initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD-12, approved by the Secretary of Commerce, and issued on February 25, 2005. Since the initial implementation of HSPD-12, federal departments and agencies have issued PIV Cards to over 96% of federal employees and contractors. Moreover, the Administration has made strong authentication an integral part of the Cybersecurity Cross Agency Goal under the GPRA Modernization Act, shown on Performance.gov. Doing so will publicly measure how PIV cards are being used to ensure that only credentialed personnel are on Federal networks.

FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications. Of particular relevance is NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, which describes technical acquisition and formatting specifications for the biometric in the PIV system, including the PIV Card itself. This document has recently been updated (Draft NIST Special Publication 800-76-2) to introduce the following biometric technologies for PIV use:

- Iris Image Records— the iris image for biometric authentication has been accepted as an additional modality to PIV credentials while the collection and use of iris recognition is optional.
- On-Card Comparison (OCC) — privacy enhancing capability in which biometric matching is executed on the PIV Card and the enrolled biometric templates cannot be read from the card. OCC also provides a means of performing card activation in lieu of the PIN.
- Facial Image –The facial image provides a cost-efficient authentication mechanism for PIV Card issuance, reissuance and verification data reset processes.
- Chain-of-Trust Records -- The "chain-of-trust" is maintained by a PIV Card Issuer and allows the holder of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication and use of the "chain-of-trust" record to personalize the new PIV Card. This capability eliminates the need for complete re-enrollment.

Draft NIST Special Publication 800-76-2 is an important step forward in the use of biometric data for PIV. NIST, as with all of its Special Publications, is engaging the public in the development and review of the document. The final SP 800-76-2 document will reflect the disposition of comments received from the first and second public comment periods and will be published once FIPS 201-2 is approved and published. If this process results in substantive changes to the draft, NIST may repeat the open comment review process to ensure all comments and issues have been adequately resolved.

National Security Presidential Directive/Homeland Security Presidential Directive (NSPD-59/HSPD-24), Biometrics for Identification and Screening to Enhance National Security

The purpose of this directive is to establish a framework to ensure that Federal executive agencies use mutually compatible methods and procedures for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under U.S. law.

The recommended executive branch biometric standards are contained in the *Registry of United States Government Recommended Biometric Standards*, which is maintained by the NSTC Subcommittee on Biometrics and Identity Management. The recommended standards include ANSI/NIST-ITL 1-2011, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* and other International Committee for Information Technology Standards (INCITS) and ISO/IEC biometric standards, which have been developed by INCITS M1, and JTC 1 SC 37. Critical identity management applications supported by these standards include: the FBI Electronic Biometric Transmission Specification; the DoD Electronic Biometric Transmission Specification; the DHS Automated Biometric Identification System (IDENT) Exchange Messages Specification; and the Terrorist Watchlist Person Data Exchange Standard (TWPDES).

NIST BIOMETRIC TESTING ACTIVITIES

Conformity assessment to biometric standards enables both providers and consumers to have confidence that biometric products or systems meet specified requirements. For IT, the three most important types of conformity assessment related testing are conformance, performance and interoperability testing. Conformance testing captures the technical description of a specification and measures whether an implementation (product, process, or service) faithfully implements the specification. Conformance testing does not completely ensure the interoperability or performance of conforming products, processes, or services. Therefore, interoperability and performance testing are also important for deployment of IT. Performance testing measures the performance characteristics of an implementation, such as its throughput or responsiveness, under various conditions. Interoperability testing tests one implementation with another to establish that they can work together properly. Testing, and ensuring the competence of bodies that do the testing, is as much of a market driver as the specific standard itself.

CONFORMANCE TESTING

Conformance testing to biometric standards captures the technical description of a specification and measures whether a biometric product's or system's implementation faithfully implements the specification. A Conformance Test Suite (CTS) is test software that is used to ascertain such conformance. NIST actively contributes to both biometric standards and biometric conformance testing methodology standards. These efforts also support users and product developers and the possible establishment of conformity assessment programs to validate conformance to biometric standards.

Conformance Testing for the ANSI/NIST-ITL Standard

Technical work started in 2006 with the release of a CTS designed to test implementations of a Biometric Application Programming Interface developed by the BioAPI Consortium and further work continued in the following years with the development of Conformance Test Architectures (CTAs) and CTSs designed to test implementations of national and international biometric data interchange formats (including the ANSI/NIST-ITL standards) and data structures that can contain biometric data of any modality (e.g., finger, face, and iris). In August 2010, NIST released an Advanced CTA and CTSs designed to test implementations of finger image and finger minutiae biometric data interchange formats specified in four American National Standards, and in 2011 we released a CTS designed to test implementations of the iris image data interchange format developed by ISO/IEC JTC 1/SC 37.

Work on the development of CTA and CTSs for the ANSI/NIST-ITL standards started in 2011 as well. NIST released a CTA/CTS for selected Record Types of ANSI/NIST-ITL 1-2007, and in 2012 we developed, in cooperation with other US Government agencies and industry, a Conformance Testing Methodology (CTM) for ANSI/NIST-ITL 1-2011 (published as NIST SP 500-295) and the associated CTA and CTS. In 2012 and early 2013, NIST released a number of CTSs for biometric international data interchange format standards and selected PIV profiles (including the PIV profile for iris data records specified in NIST SP800-76-2). The ANSI/NIST-ITL 1-2011 CTA/CTS is being updated to also support data transactions encoded in XML and data specified in the expansion of the standard. CTSs designed to test implementations of international standards encoded in XML are being developed as well. NIST is also working on developing the resources to provide support for testing laboratories and users that wish to offer remote testing of biometric data interchange formats using Web Services.

Conformance Testing for Transportation Worker Identification Credential Specifications
DHS has asked NIST to assist with its Transportation Worker Identification Credential (TWIC) specifications. The TWIC program is authorized under the provisions of the Maritime Transportation Security Act of 2002 (MTSA) (P.L. 107-295) and is a joint initiative of the Transportation Security Administration (TSA) and the U.S. Coast Guard, both under DHS. TWIC is a common identification credential for all personnel requiring unescorted access to secure areas of MTSA-regulated facilities and vessels, and all mariners must hold Coast Guard-issued credentials. TSA issued workers a tamper-resistant "Smart Card" containing the worker's biometric (fingerprint template) to allow for a positive link between the card itself and the individual. The TSA also has a requirement to establish a process to qualify products and to maintain a Qualified Technology List (QTL) of TWIC card readers for use within the TWIC program.

DHS has asked NIST to assist with the establishment of a conformity assessment framework in support of a QTL for credential verification and authentication products, to be managed by TSA. Additionally, NIST is assisting with the establishment of a testing process for qualifying products for conformity to specified standards and TSA specifications. NIST's wealth of experience with the Cryptographic Module Validation Program, smart card technology, and specific experience with the PIV card validation program, makes NIST uniquely qualified to assist TSA in establishing a conformity assessment program and a QTL for the TWIC Program.

In FY 2010, NIST set the framework for the conformity assessment process for TWIC readers and for the QTL for the credential readers that successfully passed the conformity tests and satisfy all TWIC requirements. As of the end of FY 2012, three independent testing laboratories have already been accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) to perform TWIC reader evaluations and are now available to conduct this testing for reader vendors. Card reader products from about 20 vendors have already demonstrated the ability to meet the initial requirements.

NIST is currently developing, in collaboration with our partners, the conformity assessment testing suite for credential readers. NIST will continue to support DHS's efforts by assisting in launching and managing the Conformity Assessment Program and the QTL.

PERFORMANCE AND INTEROPERABILITY TESTING
For more than a decade now, NIST has been organizing and conducting large biometric technology challenge programs and evaluations for a variety of purposes. The Multiple Biometric Grand Challenge, Face Recognition Grand Challenge and Iris Challenge Evaluation programs were conducted to challenge the face and iris recognition communities to break new ground solving research problems on the biometric frontier. The Iris Exchange (IREX) and Minutia Exchange (MINEX) programs have engaged a global community to give quantitative support for biometric data interchange standards development, to measure conformance and interoperability, foster standards adoption, and support global deployment. The Face Recognition Vendor Tests (FRVT) and the Multi-Biometric Evaluation (MBE) have been conducted to assess capabilities of face recognition prototypes for one-to-many identification and one-to-one verification. They have measured accuracy gains over the last decade that are well beyond an order of magnitude. This program has recently been expanded to test gender and age determination for emerging digital signage applications. The Speaker Recognition Evaluations (SRE) program has long challenged that community to improve speaker identification capabilities and to make implementations more robust and

versatile. The Fingerprint Technology Evaluation (FpVTE) program and Proprietary Fingerprint Template Evaluations (PFT) were developed in response to statutory mandates to established performance standards for fingerprint identification and verification.

NIST Fingerprint Minutiae Exchange (MINEX) Testing Program
NIST MINEX is an ongoing evaluation program to test fingerprint template generators and the accuracy of fingerprint matchers using interoperable standard fingerprint minutiae templates. The General Services Administration (GSA) uses the results from this interoperability testing as criteria towards certification and inclusion on the GSA Approved Products List (APL) for FIPS 201 compliant devices.

NIST Face Recognition Vendor Testing (FRVT) Program
NIST FRVT provides independent evaluations of commercially available and prototype face recognition technologies. These evaluations provide the U.S. Government with information to assist in determining where and how facial recognition technology can best be deployed, and FRVT results help identify future research directions for the face recognition community. The latest FRVT (launched July 2012) evaluated large-scale one-to-many face recognition algorithms from still face photos and (for the first time) from video, along with testing automated methods for detecting pose, expression, and gender.

NIST Iris Exchange (IREX) Testing Program
The NIST IREX testing program was initiated at NIST in support of an expanded marketplace of iris-based applications based on standardized interoperable iris imagery. The work is conducted in support of the ISO/IEC 19794-6 standard and the ANSI/NIST-ITL 1-2007 Type 17 standard.

- IREX I – (Jan 2010) Defined, tested, and validated accurate and interoperable Compact Iris Image Records for use on smart card credentials (e.g., PIV)
- IREX III – (April 2012) Evaluated large-scale one-to-many iris identification algorithms.

NIST Speaker and Language Recognition Evaluation (SLRE) Testing Program
NIST SLRE is an ongoing evaluation program to test and advance automated Speaker and Language Recognition capability through systematic evaluations and analysis that focuses research on the identified barriers that prevent the technology from reaching its full potential. The NIST project contributes to standardization efforts through the development of ANSI/NIST-ITL Type 11 standard, and is building a community-based scientific working group to develop best practices for Speaker Recognition as used for Forensic and Investigatory purposes.

- LRE-11 – (Dec 2011) Language Recognition Evaluation focusing research on distinguishing between confusable languages pairs and language dialects
- SRE-12 – (Dec 2012) Speaker Recognition Evaluation focusing research on the presence of environmental noise and capabilities with deeper speaker learning (vast amounts of training data).

Biometrics Laboratory Accreditation Program
DHS requested establishment of the Biometrics Laboratory Accreditation Program (Biometrics LAP) by NIST's NVLAP to accredit laboratories that perform conformance testing, interoperability testing, technology testing, scenario testing, and operational and usability testing for biometrics products (systems and subsystems) as defined in nationally and internationally recognized biometrics products testing standards. NIST Handbook 150-25, Biometrics Testing, presents technical requirements and guidance for the accreditation of laboratories under the NVLAP Biometrics Testing LAP. NIST Handbook 150-25 was developed with the participation of technical experts in the field of biometrics testing and was approved by NVLAP. The handbook is intended for information and use by accredited laboratories, assessors conducting on-site visits, laboratories seeking accreditation, laboratory accreditation systems, users of laboratory services, and others needing information on the requirements for accreditation under this program. There are presently two laboratories accredited under this program.

BIOMETRICS FOR THE NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE (NSTIC)

NIST is also working to advance biometrics through its work supporting implementation of the NSTIC. NSTIC is a White House initiative focused on the creation of an "Identity Ecosystem" where all Americans can choose from a variety of identity solutions that enable more secure, convenient and privacy-enhancing experiences everyplace they go online. Biometrics are one of many types of identity solutions that will play a role in the Identity Ecosystem.

NSTIC prescribes that identity solutions in this ecosystem adhere to four guiding principles. Identity solutions will be privacy-enhancing and voluntary, secure and resilient, interoperable, and cost-effective and easy to use.

Privacy is particularly important in NSTIC, and the Strategy calls for the Identity Ecosystem to offer improved privacy protection to individuals. Although individuals will retain the right to exchange their personal information in return for services they value, these protections will ensure that the default behavior of Identity Ecosystem providers is to:

- Limit the collection and transmission of information to the minimum necessary to fulfill the transaction's purpose and related legal requirements;
- Limit the use of the individual's data that is collected and transmitted to specified purposes;
- Limit the retention of data to the time necessary for providing and administering the services to the individual end-user for which the data was collected, except as otherwise required by law;
- Provide concise, meaningful, timely, and easy-to-understand notice to end-users on how providers collect, use, disseminate, and maintain personal information;
- Minimize data aggregation and linkages across transactions;
- Provide appropriate mechanisms to allow individuals to access, correct, and delete personal information;
- Establish accuracy standards for data used in identity assurance solutions;
- Protect, transfer at the individual's request, and securely destroy information when terminating business operations or overall participation in the Identity Ecosystem;
- Be accountable for how information is actually used and provide mechanisms for compliance, audit, and verification; and
- Provide effective redress mechanisms for, and advocacy on behalf of, individuals who believe their data may have been misused.

With its mission of catalyzing a marketplace of secure, privacy-enhancing identity solutions, the NSTIC National Program Office (NPO) has begun to explore how a number of authentication technologies including biometrics can be applied to meet the NSTIC vision and guiding principles. Last September, the NSTIC NPO awarded grants to five projects that will pilot NSTIC-aligned identity solutions that increase confidence in online transactions, prevent identity theft, and provide individuals with more control over how they share their personal information.

The five pilots were specifically selected for their potential to demonstrate innovative frameworks that can provide a foundation for the Identity Ecosystem, and tackle barriers that have, to date, impeded the Identity Ecosystem from being fully realized. The pilots span multiple sectors including health care, online media, retail, banking, higher education, and state and local government, and will test and demonstrate new solutions, models, or frameworks that do not exist in the marketplace today. Two of these pilots involve biometrics. One, led by the American Association of Motor Vehicle Administrators, will be demonstrating the use of signature as a biometric for authentication. A second, led by Daon, a private company, will be demonstrating the use of smartphone-based voice and facial recognition biometrics for authentication. Both pilots have a two-year period of performance and in the coming months will hit "go live" milestones.

In addition, in February, 2013, the President issued Executive Order 13636 to assist private industry and promote cyber security for the Nation's critical infrastructure owners and operators. The Executive Order directs NIST to facilitate industry-led development of a framework of best practices and voluntary cybersecurity standards for core critical infrastructure..

NIST BIOMETRIC RESEARCH ACTIVITIES ADDRESSING FUTURE CHALLENGES IN BIOMETRIC TECHNOLOGIES

The "*National Biometrics Challenge 2011*" report, published by NSTC's Subcommittee on Biometrics and Identity Management, included a few key challenges to the future application of biometric technologies, including the evolution of many of the measurement, standards and testing activities described above, as well as privacy of biometrics and usability of biometrics.

Addressing Privacy of Biometrics through Technology

Biometric technologies can be used to enhance privacy and provide a convenient authentication factor for data security. Biometrics also present some new challenges in terms of protecting personally identifiable information (PII). At NIST, we are working with the international research and standards communities to advance technical methods to safeguard and control the use of biometrics. For instance, a theft of biometric information could facilitate criminal access to accounts protected with biometrics (or multi-factor authentication). The challenge to government and industry is to create solutions that allow for the use of biometrics, while mitigating security and privacy risks (e.g., identity theft or linking user accounts) through methods such as "liveness detection" and biometric template protection.

"Liveness detection" is a method that industry is developing to counter the presentation of fake biometrics (or spoofs) at a sensor, i.e., if a biometric sample is being captured from a living subject present at the point of capture. The potential for this sort of attack is mitigated in cases in which biometrics are being collected under the supervision of an officer or other personnel. Standards, best practices, and independently evaluated techniques can enable the private sector to use a wider array of multi-factor authentication technologies to protect online transactions. A future revision of FIPS 140-2 will address this topic. In addition, NIST has successfully initiated an international standards project on anti-spoofing/liveness detection within JTC 1 SC 37 (Biometrics). This is the first standards project in this field, with the goal of strengthening the security and privacy of biometrics as an authentication factor for unattended applications. NIST is leading an international "team" of co-editors and has completed the fourth official working draft.

Another issue is that of biometric template protection (also known as cancelable or revocable biometrics). Passwords are stored and validated without being revealed through modern cryptographic means, but the same techniques cannot be used for probabilistic data, such as biometrics. Biometric template protection techniques are being developed to create biometric templates (or samples) which can be used to recognize a person but do not resemble the person's original biometric. For instance, if a template is compromised through a data breach, then the affected template can be cancelled, and a new biometric template can be issued.

NIST has collaborated with the research community through a grant to advance performance metrics for evaluating these new techniques and has held a seat (as the sole U.S. representative) on the Advisory Board of an EU research project known as the TrUsted Revocable Biometric IdeNtitiEs (TURBINE) Project .

Usability of Biometrics

The usability and ease of use of biometric systems is an overarching need and goal for deployed biometric systems within the Federal government. NIST has applied its expertise in usability and biometrics to several studies involving biometric systems in border security and airport environments, including:

- NISTIR 7540 (Sept. 2008) "Assessing Face Acquisition" – in response to a request from the Office of Biometric Identity Management (OBIM) (formerly the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program), the biometrics usability team at NIST examined the then-current OBIM face image collection process to identify any usability and human factors that may improve the existing face image capture process. The report presented results of the study that examined five usability and human factors enhancements to the then-current OBIM collection process.
- NISTIR 7504 (June 2008) "Usability Testing of Height and Angles of Ten-Print Fingerprint Capture" – this study, supported by DHS, was performed in preparation for the 10-print fingerprint capture pilot testing phase of the process through which DHS and the OBIM program transitioned from a two-print fingerprint capture process to a 10-print slap capture process. A concern was identified that the existing counters that housed the fingerprint scanners were too tall to support the capture process. The NIST Biometrics Usability team examined the impact on fingerprint capture performance based on angling of the fingerprint scanners at the existing counter heights. The study was designed to provide guidance on the "best" angle to position a fingerprint scanner given the counter heights common in U.S. ports of entry. As a result of this effort, all of the fingerprint scanners at U.S. ports of entry are now angled correctly for the collection process.

NIST's usability and biometrics research was cited in the 2010 National Academies of Science (NAS) Report, *Biometric Recognition: Challenges and Opportunities*, in which NIST is identified as one of only two organizations addressing usability in biometric systems. The NAS Report notes that "[t]he adoption of biometric systems depends on the ease with which people can use them," and calls for "…more standardized user interfaces coupled with broader human factors testing."

IMPACTS OF NIST BIOMETRIC STANDARDS, TESTING, AND RESEARCH ACTIVITIES

NIST research has provided U.S. Government agencies (whose missions' involve biometrics collection and matching) with state-of-the-art technology benchmarks and guidance. This research has helped enhance identity systems and operations including the FBI Integrated Automated Fingerprint Identification System (IAFIS) and its new Next Generation Identification (NGI) System, the DHS Automated Biometric Identification System (IDENT)/OBIM, the DoD Automated Biometric Identification System, the Department of State Biometric Visa (BioVisa) Program, and the Intelligence Community (IC) systems.

For example, the ANSI/NIST-ITL Biometrics Interchange Standard has facilitated interoperable biometric data exchange between agencies, providing a key enabling capability for the Government to implement NSPD-59/HSPD-24. NIST biometric technology evaluations in fingerprint, face, and iris have provided the Government with timely analysis of market capabilities to guide biometric technology procurements and deployments. The FBI has co-sponsored the challenge problems and evaluations and leveraged this market analysis in its acquisition of NGI system increments. NIST research assisted DHS in its transition to ten prints within OBIM where NIST conducted usability studies for slap capture of ten prints, evaluated required slap segmentation technologies, developed supporting data exchange records, and measured the interoperability between slap and rolled fingerprints. NIST is currently working with DHS to provide standards guidance, best practices, and analysis in support of designing a biometric-enabled U.S. exit process and system.

NIST has a diverse portfolio of activities supporting our Nation's biometric and identity management efforts. With NIST's extensive experience and broad array of expertise both in its laboratories and in successful collaborations with the private sector and other government agencies, NIST is actively pursuing the standards and measurement research necessary to deploy interoperable, secure, reliable, and usable identity management systems. The NIST biometrics program of work continues to support the advancement of biometrics technologies while enabling the protection of individual privacy and other legal rights under U.S. law.

Thank you for the opportunity to testify on NIST's activities in biometrics and identity management. I would be happy to answer any questions that you may have.

Mr. MICA. We will hold the questions, as I said.

We will turn next to Mr. Steven Martinez, Executive Director of the Science and Technology Branch of the FBI. Welcome, and you are recognized.

STATEMENT OF STEVEN MARTINEZ

Mr. MARTINEZ. Good morning, Chairman Mica, Ranking Member Connolly, and members of the subcommittee. I want to thank you for the opportunity to appear before the committee today and for your continued support of the men and women of the FBI.

I am pleased to describe for you today the FBIs experience in using fingerprints as an effective identification biometric so that you may consider it in the context of the issuance of Government credentials.

While the FBI has developed deep expertise in a variety of biometric modalities, the production of Government identification cards beyond our own use for physical and logical access control is not a primary area of direct FBI responsibility.

The FBI uses fingerprints in two primary ways: in conducting background checks and in criminal investigations. A criminal history record, or rap sheet, is a catalog of information taken from fingerprint submissions in connection with arrests. All arrest data, including a criminal history summary, is obtained from fingerprint submissions, disposition reports, and other information submitted by agencies having criminal justice responsibilities. The FBI also maintains a civil file of fingerprints tied to biographical data collected and submitted in matters of Federal employment, naturalization, or military service.

Fingerprints recovered from evidence found at crime scenes are processed through our Latent Print Operations Unit, or LPOU, located at the FBI Laboratory in Quantico, Virginia. These latent prints of unknown individuals are examined and used to assist in criminal investigations.

The LPOU also uses fingerprints to assist in the identification of victims from natural disasters and mass fatalities. Such events include Hurricane Katrina, the Thailand tsunami, the Oklahoma City bombing, and the attack on the USS Cole, and, most recently, the 9/11 terrorist attacks and, of course, it will be applied in the attacks in Boston.

Originally, fingerprint identification and matching were performed manually by trained fingerprint examiners in a laboratory. Today, through the use of computer technology, the practice has evolved into a highly automated and reliable process. For most of the past 14 years, more than 18,000 local, State, tribal, Federal, and international partners have been electronically submitting requests to the FBIs legacy Integrated Automated Fingerprint Identification System, or IAFIS housed and maintained by the FBIs Criminal Justice Information Services Division.

But with advances in technology, changing customer requirements, and the growing demand for IAFIS services, the FBI was compelled to create the next Generation Identification Program, or NGI, as we call it. With NGI, the FBI is dramatically improving all of the major features of IAFIS, including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems such as the biometric matching systems of the Department of Homeland Security and the Department of Defense.

NGI is being developed and deployed incrementally. The initial increment included the launch of the NGI Advanced Fingerprint Identification Technology, or AFIT, in February 2011, which replaced less capable technology within IAFIS. This enhancement provided increased processing capacity for sequence checking and image comparison. It improved search accuracy, provided a new validation algorithm for image quality, and it improved flat print screening.

NGIs system accuracy is currently measured at 99.6 percent. Prior to IAFIS, the FBI reported false matches to contributors at a rate of approximately 1 of every 50 million searches. There have been no known false matches since IAFIS went online, with nearly one-half billion fingerprint checks conducted.

NGIs second increment, the Repository for Individuals of Special Concern, or RISC, was completed in August of 2011. RISC enables mobile access to law enforcement officers nationwide through handheld devices that capture and submit fingerprints of high interest individuals and search them against the repository of wanted criminals, terrorists, and sex offenders.

As part of the third NGI increment, new capabilities in relation to latent and palm prints, rapid DHS response, and full infrastructure were completed and rolled out in May of this year. U.S. Customs and Border Protection officials at some ports of entry now have access to 10-second search of the system's full criminal master file of biometric-based criminal history information.

The fourth increment on schedule for delivery in June 2014 will complete the new system's functionality and will add two new services: Rap Back and the Interstate Photo System. The Rap Back Service will provide an ongoing status notification of any change in criminal history reported to the FBI after an individual's initial criminal history check and enrollment of their fingerprints in our files.

The final increments of NGI will include an effort to provide identification-based iris image checking, scheduled for pilot deployment in 2013, with a focus on technology refreshment as well.

Since automation through IAFIS, and now NGI, the FBI has processed more than 456 million fingerprint submissions. The current reject rate on these submissions is 3.77 percent, with most rejections being due to poor image quality or an inadequate accompanying documentation.

Strict quality control over the data enrolled in NGI, in concert with state-of-the-art automation, is key to the system's accuracy and speed. The FBI has long been a leader in the development and use of biometrics, with much emphasis on fingerprint technology. While fingerprints may be considered the most common and widely biometric modality, the FBI is actively evaluating emerging modalities, researching their accuracy, reliability, and potential suitability for the use in the lawful or constitutional performance of our mission.

This concludes my remarks, Chairman Mica, Ranking Member Connolly. I thank you for this opportunity to discuss the FBI's fingerprint and biometric programs, and I would be pleased to answer any questions you might have.

[Prepared statement of Mr. Martinez follows:]

Department of Justice

STATEMENT OF

STEVEN M. MARTINEZ
EXECUTIVE ASSISTANT DIRECTOR
SCIENCE AND TECHNOLOGY BRANCH
FEDERAL BUREAU OF INVESTIGATION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT OPERATIONS
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES

ENTITLED

"FEDERAL GOVERNMENT APPROACHES TO ISSUING BIOMETRIC IDS: PART II"

PRESENTED

JUNE 19, 2013

Statement for the Record
Steven M. Martinez
Executive Assistant Director
Science and Technology Branch
Federal Bureau of Investigation

Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives

"Federal Government Approaches to Issuing Biometric IDs: Part II"
June 19, 2013

Good morning, Chairman Mica, Ranking Member Connolly, and Members of the Subcommittee. Thank you for the opportunity to appear before the Committee today and for your continued support of the men and women of the FBI.

I was invited today to speak to the effectiveness of using fingerprints as a secure biometric technology identifier relative to the issuance of government credentials. Please let me be clear at the outset that, while the FBI has developed deep expertise in a variety of biometric modalities, production of government identification cards, beyond our own use for physical and logical access control, is not a primary area of direct FBI responsibility. Nonetheless, the FBI was an active participant in the development of Homeland Security Presidential Directive (HSPD) 12 "Policy for a Common Identification Standard for Federal Employees and Contractors" as well as NIST Special Publication 800-73 "Interfaces for Personal Identity Verification."

The FBI issues and uses public key infrastructure (PKI) enabled individual identification cards to its employees and contractors which include a personal identification number (PIN) and at least one biometric in the form of a frontal face image. The card currently does not include a fingerprint for use in "On-Card Comparison" but it is capable of doing so. The FBI does not currently employ automated biometric matching with these identification cards. For facility access, FBI police individually compare the face image stored on the card to that of the bearer. Subsequent to FBI issuance of HSPD-12 compliant identification cards the FBI has deployed highly accurate fingerprint based identity verification technology which could in future be employed with our Personal Identity Verification (PIV) cards should the need arise. I will say a bit more about our identification verification capabilities later.

As you are likely aware, fingerprinting is a time-tested method of identifying individuals based on the friction ridge patterns and minutiae found on their fingertips. As a general matter, no two persons have been found to possess the exact same sets of fingerprints and those fingerprints are persistent throughout one's lifetime. Even identical twins have different fingerprints. Fingerprints can be recorded on a standard fingerprint card or recorded electronically. By comparing known fingerprints to collected fingerprints, officials can establish the identity of a person in a quick manner.

History

The use of fingerprint identification in the United States dates back to 1902. The New York Civil Service Commission established the practice of fingerprinting applicants to prevent them from having better qualified persons take their tests for them. The New York state prison system began to use fingerprints for the identification of criminals in 1903. In 1904 the fingerprint system accelerated when the United States Penitentiary at Leavenworth, Kansas, and the St. Louis, Missouri, Police Department both established fingerprint bureaus. During the first quarter of the 20th century, more and more local police identification bureaus established fingerprint systems. The growing need and demand by police officials for a national repository and clearinghouse for fingerprint records led to an Act of Congress on July 1, 1921, establishing the Identification Division of the FBI. In 1933, the United States Civil Service Commission, known today as the Office of Personal Management, submitted 140,000 government employees' fingerprints and applications to the FBI precipitating the creation of the Civil Identification Section. In 1992, the FBI Identification Division was restructured as the Criminal Justice Information Services Division, or CJIS, now located in Clarksburg, West Virginia.

Use of Fingerprints

The FBI uses fingerprints in two primary ways: background checks and criminal investigations.

A criminal history record, or a "rap sheet", is a catalog of information taken from fingerprint submissions in connection with arrests and in some instances, federal employment, naturalization, or military service. When fingerprints are related to an arrest, the Criminal History Summary includes name of the agency that submitted the fingerprints to the FBI, the date of the arrest, the arrest charge, and the disposition of the arrest. All arrest data included in a Criminal History Summary is obtained from fingerprint submissions, disposition reports, and other information submitted by agencies having criminal justice responsibilities.

Fingerprints recovered from evidence found at crimes scenes are processed through our Latent Print Operations Unit (LPOU) located at the FBI Laboratory in

Quantico, VA. These prints, typically referred to as latent prints, are examined and used to assist in criminal investigations. The LPOU also uses fingerprints to assist in the identification of victims from natural disasters and mass fatalities. Such events include: Hurricane Katrina, the Thailand Tsunami, the Oklahoma City bombing, TWA Flight 800, the Space Shuttle Challenger explosion, the attack on the USS *Cole*, and the 9/11 terrorist attacks.

Modern Fingerprint Matching as a Criminal Justice Information Service

Originally, fingerprint identification and matching were performed manually by trained fingerprint examiners in a laboratory. Today, the practice has evolved through the use of computers into a highly automated and reliable process. Currently, more than 18,000 local, state, tribal, federal, and international partners electronically submit requests to the FBI's Integrated Automated Fingerprint Identification System (IAFIS) housed and maintained by the CJIS Division. However, advances in technology, customer requirements, and the growing demand for IAFIS services, compelled the FBI to create the Next Generation Identification or NGI Program in order to bring identification services to the next level. The NGI Program is advancing the FBI's biometric identification and investigation services by providing an incremental replacement of current IAFIS technical capabilities, while introducing new biometric functionality. With NGI, the FBI is dramatically improving all of the major features of the current IAFIS, including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems, such as the biometric matching systems of the Department of Homeland Security (DHS) and the Department of Defense.

NGI is being developed and deployed incrementally. The initial increment included the launch of the NGI Advanced Fingerprint Identification Technology (AFIT) on February 25, 2011, which replaced the Automated Fingerprint Identification System (AFIS) segment of the IAFIS and provided the following: faster algorithm processing; increased "lights out" processing (without staff intervention) for sequence check and image comparison; improved search accuracy; new validation algorithm for image quality and sequence checks; and improved flat print searching. Enhancements to the system have decreased the transaction rejection rate due to a better ability to process poor image quality probe and exemplar submissions. The NGI accuracy is currently measured at 99.6 percent. Prior to IAFIS the FBI had rare false matches reported to contributors, approximately 1 per 50,000,000. There have been no known false matches since IAFIS initial operability with nearly ½ billion fingerprint checks conducted. Further, these technology advancements have also provided the ability for FBI to respond to criminal submissions with an average of only 8 minutes, 52 seconds.

NGI's second increment, the Repository for Individuals of Special Concern (RISC) was completed in August 2011, and provides mobile access for law enforcement officers nationwide through hand-held devices that submit fingerprints of high interest individuals against a repository of wanted criminals, terrorists, and sex offenders. Rapid responses are received in the field in a red, yellow, or green format. Eleven states are currently participating in the RISC and nearly 800,000 RISC transactions have been processed to date.

Capabilities in relation to latent and palm prints, rapid DHS response, and full infrastructure were rolled out as part of the third increment, completed in May of this year (2013). All contributors immediately benefited from 3 times increased accuracy, and now have access to a National Palm Print Repository, which continues to grow. Some U.S. Customs and Border Protection, Ports of Entry Primary, now have access to a 10-second search of the system's full Criminal Master File of biometric-based criminal history information. The expanded cascaded searches of the Unsolved Latent File have already produced potential matches.

The fourth increment, expected to be delivered in June 2014, will include replacing the legacy system functionality and adding new services of Rap Back and the Interstate Photo System. The Rap Back Service will provide an on-going status notification of any change in criminal history (e.g., an arrest or a conviction) reported to the FBI after an individual's initial criminal history check. This service can be used both for noncriminal justice applicants, employees, volunteers, licensees, etc., and for individuals under criminal investigation or under the supervision of criminal justice agencies. The Interstate Photo System Facial Recognition Pilot is a collaboration among the FBI and state law enforcement agencies to assess NGI face search capabilities on real data. Authorized law enforcement partners can search more than 15.2 million criminal face images, or "mug-shots."

The final increments of NGI will include an effort to provide identification based on iris images, scheduled for pilot deployment in 2013, and a focus on technology refreshment.

Since automation through IAFIS, the FBI has processed more than 456 million fingerprint submissions. The current reject rate on these submission is 3.77% (Note: average error rate over the last 13 months), with most of these (3/4) due to poor image quality.

Other Biometrics

The FBI has long been a leader in the development and use of biometrics. While fingerprints may be considered the most common and widely used biometric modality, other biometrics await just beyond the horizon and the FBI is actively researching their accuracy, reliability and potential suitability in the lawful and Constitutional performance of our mission. The FBI is, for example, a recognized leader in forensic deoxyribonucleic acid (DNA) identification and has been a leader in the development of Rapid DNA identification equipment to allow use of DNA as a biometric element of identification during the criminal booking process. As just mentioned, face identification services, matching police photo submissions to mug shots collected during the criminal booking process is a planned capability of the Next Generation Identification (NGI) System which is currently under development. Iris has proven to be an effective modality for prisoner custodial management and transfer applications. NGI is developing a pilot project that will assess the cost effectiveness of iris matching as an NGI service. The FBI also conducts forensic speaker identification analyses. To further explore and advance the use of new and enhanced biometric identity management technologies and capabilities, the FBI created the Biometric Center of Excellence (BCOE), headquartered at the CJIS Division in Clarksburg, WV.

I'd like to address briefly some of the other biometric modalities, beyond fingerprints, that the FBI is evaluating.

The computer-based facial recognition industry has made useful advancements in the past decade, facilitated in no small measure through the standards of the National Institute of Standards and Technology (NIST), DHS, and the FBI. However, the need for higher accuracy remains. Through the determination and commitment of industry, government evaluations, and organized standards, growth and progress continue raising the bar for this technology.

Palm print identification, just like fingerprint identification, is based on the aggregate of information presented in a friction ridge impression. This science is still relatively new and there have been large advances with continued studies and research.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent since 1994, therefore a need for continued research and testing remains. DHS and the Intelligence Technology Innovation Center co-sponsored a test of iris recognition accuracy, usability, and interoperability referred to as the Independent Testing of Iris Recognition Technology.

Speaker recognition relies on voice recognition (not to be confused with "speech recognition,") which recognizes words as they are articulated and does not yield a biometric signature). The speaker recognition process relies on both the physical structure of an individual's voice and the individual's behavioral characteristics. Both National Security Agency and NIST are committed to further research and with their collaboration, speaker recognition will continue to evolve.

DNA is another popular biometric modality. A DNA profile comes from biological samples such as blood, saliva, hair, semen, or tissue. The benefit of using DNA as a biometric identifier is the level of accuracy offered. For example, with 13 different bands used today, the chance of two individuals sharing the same DNA profile is rarer than one in a 100 billion.

Finally, the FBI's BCOE will be looking at the potential of emerging biometric technology to allow federal and local law enforcement partners to increase their identity management capabilities. The BCOE will also work on developing and enhancing other potential new biometric technologies including footprint and hand geometry, gait recognition.

Conclusion

Chairman Mica and Ranking Member Connolly, I thank you for this opportunity to discuss the FBI's fingerprint and biometric programs.

I look forward to any questions that you may have.

Mr. MICA. Thank you. As we said, we will hear from all the witnesses.

We will hear from John Allen, who is the Director of Flight Standards Service with FAA next. You are recognized. Welcome.

STATEMENT OF JOHN ALLEN

Mr. ALLEN. Good morning, Chairman Mica and Ranking Member Mr. Connolly. Thank you for the opportunity to appear before you today on the issue of incorporating biometric data into pilot certificates.

The FAA has responsibility for issuing 23 different types of airman certificates. In addition to pilot certificates, these include certificates for mechanics, dispatchers, parachute riggers, and air traffic controllers. The agency also issues certificates for flight attendants. There are approximately 837,000 active pilot certificate holders.

Historically, the primary function of these pilot certificates was simply to document that its holder meets the aeronautical knowledge and experience standards established for both the certificate level and any associated ratings.

Although pilot certificates have not been intended for identification verification purposes, the FAA has a long history of responding to law enforcement interest in enhancing airman certificates. Pursuant to the Drug Enforcement Administration Act of 1988, for example, the FAA began the process of phasing out paper certificates and replacing them with security-enhanced plastic.

Since April 2010, all pilots have been required to have the new plastic certificates, and holders of the remaining airman certificate types, such as mechanics and dispatchers, were required to have these plastic certificates by March 31st, 2013. These plastic certificates include tamper-and counterfeit-resistant features such as micro printing, a hologram, and a UV-sensitive layer.

Additionally, the FAA has taken other steps to meet law enforcement concerns. Since 2002, the FAA has required pilots to carry a valid Government issue photo ID, as well as a pilot certificate, in order to exercise the privileges associated with the certificate. This allows an FAA inspector or a fixed-based operator that rents airplanes to confirm both the individual's identity and his or her pilot credentials.

In 2004, Congress directed the FAA to develop tamper-resistant pilot certificates that include a photograph of the pilot and are capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier the FAA administrator considers necessary. I want to emphasis the FAA had already met some of these requirements when we began issuing the tamper-and counterfeit-resistant certificates in 2003.

To address the remaining requirements, the FAA was required to initiate a rulemaking. We did so in November 2010, and while the agency was reviewing the hundreds of comments received on that notice of proposed rulemaking, the FAA Modernization and Reform Act of 2012 became law.

Section 321 of that Act requires that pilot certificates not only contain photographs, but also be smart cards that can accommodate iris and fingerprint biometrics, and are compliant with specific standards for processing through security checkpoints and to airport sterile areas. The FAAs NPRM did not contemplate these additional features.

Because the Section 321 requirements were not within the scope of the previous NPRM, the agency was required to initiate another rulemaking in order to comply with the congressional directives. Currently, we are developing a notice of proposed rulemaking to issue smart card pilot certificates that can accommodate a photograph and other biometric data.

In addition, we are analyzing the costs and benefits of various alternatives to meet this statutory mandate. To justify imposing a new cost on pilots, we must carefully consider the benefits of improved pilot certificates, and if pilot certificates with embedded biometrics are intended to permit airport access or increased security, we must coordinate with the Department of Homeland Security and TSA, who develop standards for airport access and security.

Further, the FAA must coordinate our efforts with the National Institute of Standards and Technology, which is in the process of establishing standards for use of iris biometric data. It is essential to identify and quantify the benefits of biometric enhancements and work with other Federal agencies as we move forward. The FAA must ensure we are not duplicating effort or imposing an undue burden on the public. We must also coordinate with airlines, industry trade associations, and organizations representing individual pilots through the FAAs aviation rulemaking committee process.

We are working hard to accomplish the goals outlined by Congress and we are in the final stages of preparing a report to Congress. We believe this report will assist Congress in assessing the future use and inclusion of biometric data in pilot certificates. We look forward to working with you and in collaboration with other agencies as our efforts progress.

This concludes my prepared remarks. I will be happy to take questions as you wish. Thank you.

[Prepared statement of Mr. Allen follows:]

STATEMENT OF JOHN ALLEN, DIRECTOR OF FLIGHT STANDARDS SERVICE, FEDERAL AVIATION ADMINISTRATION, BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, SUBCOMMITTEE ON GOVERNMENT OPERATIONS, ON THE INCLUSION OF BIOMETRIC IDENTIFIERS ON GOVERNMENT ID CARDS, June 19, 2013.

Chairman Mica, Congressman Connolly, Members of the Subcommittee:

Thank you for the opportunity to appear before you today on the issue of incorporating biometric data into pilot certificates. I know this issue has been of significant interest to Chairman Mica. The FAA previously appeared before the House Committee on Transportation and Infrastructure on this issue under Chairman Mica's leadership in 2011.

The FAA has responsibility for issuance of 23 different types of airman certificates. In addition to pilot certificates, these include certificates for mechanics, dispatchers, parachute riggers, and air traffic controllers. The agency also issues certificates to flight attendants. There are approximately 837,000 active pilot certificate holders.

Historically, the primary function of a pilot certificate was simply to document that its holder meets the aeronautical knowledge and experience standards established for both the certificate level and any associated ratings.

Even before the September 11 terrorist attacks, the FAA was responding to law enforcement interest in enhancing the security of airman certificates. Pursuant to the Drug Enforcement Administration (DEA) Act of 1988, for example, the agency began the process of phasing out paper certificates and replacing them with plastic. Since April 2010, all pilots have been required to have the new plastic certificates. Holders of the remaining airman certificate types –

that is, navigators, mechanics, dispatchers, etc. – were required to have a security-enhanced plastic certificate by March 31, 2013. As of March 31, all airman certificate holders, including pilots, have plastic certificates that incorporate tamper- and counterfeit-resistant features. These include micro printing, a hologram, and a UV-sensitive layer.

As you know, the Intelligence Reform and Terrorism Prevention Act (IRTPA) that the Congress passed in 2004 requires additional security measures for pilot certificates. Specifically, the IRTPA directed the FAA to develop tamper-resistant pilot certificates that include a photograph of the pilot and are capable of accommodating a digital photograph, a biometric identifier, or any other unique identifier the FAA Administrator considers necessary.

The FAA had already met some of these requirements when it began issuing tamper- and counterfeit-resistant certificates in 2003. To address the remaining requirements, the FAA was required to initiate a rulemaking. Before I discuss the rulemaking effort, let me note that the FAA chose to use a digital photo as the method of complying with IRTPA. However, we are working closely with the Transportation Security Administration (TSA) on measures that will provide additional security enhancements not only to pilot certificates, but also to other types of airman certificates.

The FAA has also taken other steps to meet law enforcement concerns. Since 2002, the FAA has required pilots to carry a valid Government issued photo ID as well as a pilot certificate in order to exercise the privileges associated with the certificate. This allows an FAA inspector or a fixed-base operator that rents airplanes to confirm both the individual's identity and his or her pilot credentials.

In response to IRPTA, the FAA initiated a rulemaking to require digital photographs to appear on pilot certificates. While the agency was reviewing the hundreds of comments received on the Notice of Proposed Rulemaking (NPRM) the FAA Modernization and Reform Act of 2012 became law. Section 321 of that Act requires that pilot certificates not only contain photographs, but also be smart cards that can accommodate iris and fingerprint biometric identifiers and are compliant with FIPS-201 or Personal Identity Verification-Interoperability Standards (PIV-I) for processing through security checkpoints into airport sterile areas. The FAA's NPRM did not contemplate those additional features.

Because the requirements of Section 321 were not within the scope of the previous NPRM, the agency was required to initiate another rulemaking in order to comply with congressional directives. The rulemaking process requires the FAA to propose requirements for an applicant to obtain and use an improved pilot certificate, analyze the costs and benefits of those requirements, consider public comments to the proposal, and issue final requirements. In accordance with this process, the FAA is developing a notice of proposed rulemaking to issue smart card pilot certificates that can accommodate a photograph and other biometric data.

The cost of this transition has not yet been determined, but analysis of the costs and benefits of various alternatives to meet the statutory mandate is underway.

To justify imposing a new cost on pilots, we must carefully consider the benefits of improved pilot certificates. If pilot certificates with embedded biometrics are intended to permit airport access or increase security, we must coordinate with the Department of Homeland Security (DHS) and the TSA, which develop standards for airport access and security.

There are also implications for multiple government agencies. The National Institute of Standards and Technology (NIST) is in the process of a rulemaking that will establish standards to enable the use of iris biometric data, but has not yet established this standard. That impacts the FAA, since the agency seeks to avoid duplicating, interfering with, or superseding efforts by other federal agencies with respect to standards or implementation. To address and coordinate these issues, and to evaluate quantifiable benefits regarding how this technology might advance each agency's mission, the FAA is participating in an interagency working group that includes DHS through the TSA, as well as NIST. In addition to avoiding duplication or conflicting standards that would impose an undue burden on pilots, the working group seeks to learn from best practices in other agencies. One such example is the DHS Global Online Enrollment System (GOES) for managing the U.S. government's trusted traveler programs.

It is therefore essential to identify and quantify the benefits of biometric enhancements as we move forward.

Understanding how to maximize the use of biometric data to ensure the security of the pilot community, to enhance overall aviation security in a way that does not create duplication or impose an undue burden, and to craft a rule that can meet the statutory mandates, while accommodating rapidly evolving technologies. It will also require a government working group (through FAA's Aviation Rulemaking Committee process) to coordinate with airlines, industry trade associations, and organizations representing individual pilots.

We are working hard to accomplish the goals outlined by Congress. In consultation with other agencies, the FAA is in the final stages of preparing a report to Congress. We believe this report will assist Congress in assessing the future use and inclusion of biometric data in pilot certificates. We look forward to working with you, and in collaboration with other agencies, as our efforts progress.

This concludes my prepared remarks. I will be happy to take questions at this time.

Mr. MICA. We will get back to questions.

Ms. Colleen Manaher is the Executive Director of Planning, Program Analysis, Evaluation with Customs and Border Patrol.

Welcome, and you are recognized.

STATEMENT OF COLLEEN MANAHER

Ms. MANAHER. Good morning, Chairman Mica, Ranking Member Connolly, and distinguished members of the Subcommittee. Thank you for this opportunity to appear before you on behalf of the dedicated men and women of the U.S. Customs and Border Protection to discuss our Trusted Traveler Programs and the use of biometric information to enhance the security of these programs.

As the unified border security agency of the United States, CBP is responsible for securing our Nation's borders, while facilitating the flow of legitimate trade and travel that is vital to our Nation's economy. CBP operates at more than 320 ports of entry and processes nearly 1 million travelers every day as they enter the United States.

From 2009 to 2012, the volume of international air travelers has increased by 12 percent and is projected to increase 4 to 5 percent each year for the next five years. CBP continues to address the security elements of its mission, while meeting the challenges of increasing volumes of travel in the land, air, and sea environments. We do this by implementing multiple layers of security throughout the entire supply chain of goods and throughout the entire transit sequence for people.

We accomplish our mission of expediting trade and travel by separating the knowns from the unknowns. This risk-based segmentation allows us to facilitate the entry of legitimate trade and travel. Twenty million of these known documents have been issued by DHS, our partners at the Department of State, by four of our States, four provinces in Canada, and two U.S. Native American tribes. By knowing the holder of these 20 million documents, CBP can focus its resources on travelers and traders that are unknown, with the goal of stopping illegitimate trade and travel.

I would like to share just a bit more detailed information with you on DHSs flagship credentialing program, CBPs Trusted Traveler Program, which had been essential to our risk-based approach to expedite the flow of travelers into the United States. It provides expedited processing upon arrival for pre-approved, low-risk participants through the use of secure and exclusive dedicated lanes and automated kiosks.

Our Trusted Traveler Program issues secure documents in accordance with the best practices consistent with international standards, applies rigorous biographic and biometric vetting procedures, all of which increases our confidence in a program that provides a secure service when time is valuable. We simply know far more about these travelers than anyone else.

CBP operates four Trusted Traveler Programs: SENTRI for our land border crossings along the southern border; NEXUS for our air, land, and marine environments along the northern border; FAST for low-risk commercial carriers and truckers; and Global Entry for our international air travelers.

SENTRI, the Secure Electronic Network for Travelers Rapid Inspection Program was established in 1995 and has grown to include over 20 vehicle lanes at the 12 largest southern border crossings along the U.S.-Mexican border. SENTRI pedestrian crossing is also available at several locations. SENTRI members currently account for 14 percent of all cross-border traffic. Approximately 58,000 travelers a day use the SENTRI lanes.

NEXUS is a partnership program between the United States and Canada, and provides for the expedited travel for air, land, and the marine environment along the northern border. A NEXUS applicant also undergoes an interview conducted by officers by both CBP and the Canada Border Services Agency. NEXUS is the only CBP Trusted Traveler Program that requires the collection and use of an iris scan for travelers wishing to use the program at Canadian pre-clearance locations.

The Free and Secure Trade Program, FAST, is a commercial clearance program for known motorist shipments entering the United States from Canada and Mexico. FAST allows for expedited processing for commercial carriers to include the truck driver. Participation in FAST requires that every link in the supply chain, from manufacturer to carrier to driver to importer be certified under the Customs Trade Partnership Against Terrorism, or CTPAT, program.

Global Entry is an expedited customs clearance program for pre-approved, low-risk air travelers entering the United States without routine CBP questioning, bypassing the regular passport control cues and, instead, use an automated kiosk at over 34 designated airports, accounting for 98 percent of the arriving international travelers.

Advanced technology is the critical element of the Trusted Traveler Programs. In the land border environment, the implementation of the Western Hemisphere Travel Initiative involves a substantial technology investment that continues to provide both facilitation and security benefits. Today, as a result of that Initiative, more than 20 million RFID-enabled technology documents have been issued. These documents represent the ultimate in security feature, as they can be verified electronically in real-time back to the issuing authority to establish identity and citizenship. They also reduce the average vehicle processing time by 20 percent.

RFID technology has also increased CBPs capability to query national law enforcement databases, including the U.S. Government's terrorist watch list. Today, CBP is able to perform law enforcement queries for 97 percent of travelers at the land border, compared to only 5 percent in 2005.

More than 1.9 million people, including 425,000 new members this year, have enrolled in the Trusted Traveler Program. Fees range from $50 to $122 for a five-year membership, which covers the direct cost affiliated with these programs. The time and resource savings for CBP are considerable. For example, as of May 2013, Global Entry kiosks have been used 4.6 million times.

When that many passengers use Global Entry, it frees up the equivalent of 18 CBP officers to focus on other mission-critical work. The time savings are extended to travelers as well. Global entry has reduced wait times for members more than 70 percent, compared to the general process. More than 75 percent of the travelers using Global Entry are processed in less than 5 minutes. In fiscal year 2012, the average NEXUS vehicle processing time was only 20 seconds.

To counter the threat of terrorism, secure our borders, while expeditiously facilitating travel and trade, CBP relies on a balanced mix of professional law enforcement personnel, advanced technologies, and innovative programs. CBP has made significant progress in securing the borders through a multi-layered approach using a variety of tools at our disposal.

We will continue to enhance and expand our Trusted Traveler Program, which expedites the processing of known and low-risk travelers as we focus our attention on the high-risk travelers. We will remain vigilant and focus on building our approach to position CBPs greatest capability to combat the greatest risks that exist today.

Chairman Mica, Ranking Member Connolly, thank you for this opportunity to testify about the work of CBP and our efforts. Thank you.

[Prepared statement of Ms. Manaher follows:]

STATEMENT FOR THE RECORD

Colleen Manaher
Executive Director, Planning, Program Analysis, and Evaluation
Office of Field Operations

U.S. Customs and Border Protection
Department of Homeland Security

BEFORE

House Oversight and Government Reform
Subcommittee on Government Operations

ON

"Federal Government Approaches to Issuing Biometric IDs: Part II"

June 19, 2013
Washington, DC

INTRODUCTION

Chairman Mica, Ranking Member Connolly, Members of the Subcommittee, it is a privilege and an honor to appear before you to discuss the work of U.S. Customs and Border Protection (CBP), particularly with regard to CBP's development of the minimum standards and best practices for the issuance of cross border travel documents through the Western Hemisphere Travel Initiative (WHTI), CBP's Trusted Traveler Programs and the use of biometrics to secure these programs.

As America's frontline border agency, CBP's priority mission is to protect the American public, while facilitating lawful travel and trade. To do this, CBP has deployed a multi-layered, risk-based approach to enhance the security of the people and goods entering the United States. This layered approach to security reduces our reliance on any single point or program that could be compromised.

On a typical day, CBP welcomes nearly a million travelers at our air, land, and sea ports. The volume of international air travelers increased by 12 percent from 2009 to 2012 and is projected to increase 4 to 5 percent each year for the next five years[1]. CBP continues to address the security elements of its mission while meeting the challenge of increasing volumes of travel in air, land, and sea environments, by assessing the risk of passengers from the earliest, and furthest, possible point, and at each point in the travel continuum.

Working with our partners, CBP secures our Nation's borders by employing and enhancing our layers of defense throughout the entire supply chain (for goods) and transit sequence (for people) -- starting from their points of origin, transit to the United States, to their arrival and entry at our ports of entry. These layers rely upon increased intelligence and risk-management strategies regarding the movement and flow of both travelers and trade. Risk segmentation, separating the "knowns" from the "unknowns" allows us to enhance security by focusing more attention on stopping illegitimate trade, while at the same time facilitating legitimate travel and commerce.

[1] U.S. Commerce Department Forecast of Growth in International Travel to the United States Through 2016. http://www.commerce.gov/news/press-releases/2012/04/23/us-commerce-department-forecasts-growth-international-travel-united-s.

More than 1.9 million people, including more than 425,000 new members this fiscal year, have enrolled in Trusted Traveler Programs, which allow expedited clearance for pre-approved, low-risk travelers upon arrival in the United States. These trusted travelers carry credentials that meet or exceed the International Organization for Standardization security standards and exceed the best practices for protection of personal identification documents.

Western Hemisphere Travel Initiative (WHTI)

In 2009, CBP implemented a key 9/11 Commission recommendation through WHTI and established the minimum requirements for cross-border travel documents with the states, tribes and Canada. This program involved a substantial technology investment in the land border environment that continues to provide both facilitation and security benefits. Today, as a result of WHTI, more than 20 million Radio Frequency Identification (RFID) technology-enabled travel documents have been issued. These documents are more secure, as they can be verified electronically in real-time back to the issuing authority to establish identity and citizenship; they also reduce the average vehicle processing time by 20 percent.

A direct result of the increased use of RFID-enabled secure travel documents is CBP's capability to increase the national law enforcement query rate, including queries against the terrorist watch list, to more than 98 percent. By comparison, in 2005, CBP performed law enforcement queries in the land border environment for only 5 percent of travelers.

OVERVIEW OF TRUSTED TRAVELER PROGRAMS

CBP operates four international trusted traveler programs offering expedited processing for pre-identified, lower risk populations. These programs improve security by increasing efficiencies in allocating screening resources, and facilitate legitimate trade and travel. Membership in these programs is valid for five years, and the application process, membership requirements, and standard of vetting are the same.

Applicants who voluntary participate in the program undergo the following: a biographical background check against criminal, law enforcement, customs, immigration, and terrorist indices; a 10-fingerprint law enforcement check; and a personal interview with a CBP officer.

Fingerprints are checked against the FBI database for criminal history and also are run against and stored in the DHS Automated Biometric Identity System, IDENT, which is used to perform the biometric match during the primary inspection. CBP also conducts recurrent vetting checks every 24-hours. As a result of the recurring vetting, if an individual is found to no longer be eligible to participate in the program the individual's membership will be immediately revoked and subsequently they will be notified of the revocation.

Once enrolled, applicants are issued a RFID-enabled card that identifies their record and status in CBP's database upon arrival at a port. There are many security features on the Trusted Traveler cards. The personal data on the cards are laser engraved. The documents use a combination of printed and electronic security features. Some of the printed features can be seen, others cannot. An antenna and RFID chip embedded within the card help to verify the identity of the bearer to Customs and Border Protection Officers while optical security features help officers quickly validate that both the traveler and card are authentic.

Secure Electronic Network for Travelers Rapid Inspection (SENTRI)

The Secure Electronic Network for Travelers Rapid Inspection, also referred to as the SENTRI program, offers pre-approved, low-risk travelers expedited entry into the U.S. through designated lanes at the U.S.-Mexico land border ports. In addition to the standard vetting process, and an RFID enabled card, the SENTRI program requires a vehicle or motorcycle inspection to take place. A sticker decal is issued once complete. SENTRI users have access to specific, dedicated primary lanes into the U.S.

SENTRI was first implemented at Otay Mesa, CA, in 1995, and has grown to include the ten largest southern border POEs along the U.S.-Mexico border. SENTRI members currently account for 19 percent of all cross SWB traffic. The fee for SENTRI is $122.25.

NEXUS

NEXUS is a bilateral program with the Canada Border Services Agency (CBSA), which offers pre-approved, low-risk travelers expedited travel between the U.S. and Canada through designated lanes and kiosks at the land border and all Canadian preclearance airports, as well as in the marine environment for pleasure boaters. NEXUS identifies low-risk travelers through: a complete biographic check; an interview with a CBP officer and a CBSA officer; and a biometric (fingerprint) criminal history check.

Once identified as low-risk, applicants are enrolled in NEXUS and given a RFID-enabled card that is unique to the traveler. The card allows the traveler to use dedicated primary lanes at land border POEs reserved for NEXUS member use. At the Canadian airports that have NEXUS Air kiosks, passengers use kiosks instead of dedicated lanes; and iris scans identify low-risk travelers. NEXUS Air kiosks uses a biometric identifier (iris) in place of RFID-enabled cards like at the land border dedicated lanes. At the time of enrollment, travelers qualify for trusted traveler status in all modes of travel (air, sea and land).

In FY 2012, the average NEXUS program lane processing time, 20 seconds, was two and a half times faster than vehicles processed at general lanes crossing the northern border (general lane times along the northern border average 50 seconds per vehicle). For FY 2012, the NEXUS program lanes produced an inspection time savings equivalent to 24 CBP officers. The fee for NEXUS is $50.

Free and Secure Trade (FAST)

CBP's Free and Secure Trade, more commonly known as FAST is the cargo equivalent of the SENTRI and NEXUS facilitative programs. Through FAST, importers, commercial carriers, truck drivers and manufacturers who enroll in the program and meet agreed upon security criteria, including participation in the C-TPAT program, are granted expedited clearance at a POE. Using electronic data transmission and transponder technology, CBP expedites clearance of approved trade participants. FAST supports a more secure supply chain and enables CBP to focus security efforts and inspections on high-risk commerce, where the attention is most needed. The fee for FAST is $50.

GLOBAL ENTRY (GE)

GE, CBP's newest trusted traveler program, which launched in 2008, is aimed at facilitating low-risk travelers in the air environment. CBP designed GE for expedited clearance of pre-approved low-risk air travelers into the U.S. using automated kiosks, placed in the Federal Inspection Services area of each identified airport, allowing GE enrolled travelers to bypass queues and process through Passport Control without having to see a CBP officer. GE facilitated entry into the U.S. is especially beneficial to frequent international flyers. Currently, GE is available at Atlanta, Baltimore, Boston, Charlotte, Chicago, Dallas/Ft. Worth, Denver, Detroit, Ft. Lauderdale, Guam, Honolulu, Houston, John Wayne Orange County, Las Vegas, Los Angeles, Miami, Minneapolis, Newark, New York (JFK), Orlando, Philadelphia, Phoenix, Portland (OR), Raleigh-Durham, San Antonio, Salt Lake City, Sanford (FL), San Juan, San Diego, San Francisco, Saipan, Seattle, Tampa, and Washington Dulles airports. GE is also available at all eight Canadian preclearance sites - Calgary, Edmonton, Halifax, Montreal, Ottawa, Toronto, Vancouver, and Winnipeg; at two preclearance sites in Ireland - Dublin and Shannon; and two U.S. territory sites - Guam and Saipan.

GE membership is currently available to U.S. citizens, U.S. lawful permanent residents (LPRs), and Mexican nationals. Canadian citizens and residents may enjoy GE benefits through membership in the NEXUS program. Additionally, in a joint arrangement with the Netherlands, CBP allows Dutch citizens to participate in GE, and U.S. citizens to participate in the Dutch trusted traveler program, Privium. A joint arrangement with South Korea allows Korean citizens to participate in GE, and U.S. citizens to participate in the South Korean Trusted Traveler program, the Smart Entry System. CBP is operating pilot programs with Germany, Qatar, and the United Kingdom, allowing limited numbers of their citizens to participate in Global Entry. Once CBP enters into a bilateral agreement, a pilot may be conducted at the request of the partner country to test the application and vetting systems of the partner country before the program is formally launched. GE members use automated kiosks located in the Federal Inspection Services (FIS) area of each program airport. Kiosk transactions are initiated by inserting the member's travel document (passport or lawful permanent resident card) into the document reader. Through fingerprint biometrics and passport or LPR card data, the GE kiosk: validates membership eligibility; performs real time law enforcement database queries; and allows the traveler to complete CBP Declarations questions via touch screen. Upon successful completion of the GE process at the kiosk, the traveler will be issued a transaction receipt and directed to baggage claim and the exit, unless chosen for a selective or random secondary referral. Global Entry Members are also issued a card, however this is not for use of the kiosk. These cards may be used at the land borders. The cards allow GE members to make use of the NEXUS and SENTRI lanes when travelling into the U.S. via the land borders.

To date, more than 718,000 travelers have enrolled in the Global Entry program. Global Entry has reduced average wait times for Global Entry users by more than 70 percent for the participants, with more than 75 percent of travelers using Global Entry processed in less than five minutes. The 283 Global Entry kiosks have been used nearly 5 million times, equal to approximately 83,300 CBP inspectional processing hours. These hours are then expended on the normal passenger processing, helping to reduce overall wait times. The fee for Global entry is $100.

COSTS VS COST SAVINGS

CBP is conducting a new fee study, expected to be complete by the end of this year, for its Trusted Traveler Programs. Once the fee study is complete, DHS will publish a Federal Register Notice, which will include a comment period. To support Trusted Traveler Programs, CBP is authorized to use approximately $6 million in appropriated funding each fiscal year. Appropriated funds are complemented with over $30M in revenues (user fee collections fluctuate due to economic factors and cycles of enrollment renewals) generated by enrollment fees. Combined resources are used to fund staff vetting applications, and equipment and maintain information systems. In addition, the cost avoidance of these programs in terms of inspectional hours saved due to the increased efficiencies and faster processing times is the equivalent of $21.6 million, or 220,860 inspectional hours saved.

CONCLUSION

To counter the threat of terrorism and secure our borders, while expeditiously facilitating legitimate trade and travel, CBP relies on a balanced mix of professional law enforcement personnel, advanced technologies and modernized facilities and infrastructure both at and between the ports of entry. With the support of Congress, CBP has made significant progress in securing the borders through a multi-layered approach using a variety of tools at our disposal. CBP will continue to work within DHS and with our federal, state, local, tribal, and international partners, to strengthen border security. We must remain vigilant and focus on building our approach to position CBP's greatest capabilities to combat the greatest risks that exist today, to be prepared for emerging threats, and to continue to build a sophisticated approach tailored to meet the challenges of securing a 21st century border.

We are continuing to enhance and expand our trusted traveler programs, which expedite the processing of known, low-risk travelers so that we can better focus our attention on higher-risk, unknown travelers.

Chairman Mica, Ranking Member Connolly, Members of the Subcommittee, thank you for this opportunity to testify about the work of CBP and our efforts in securing our borders. We look forward to answering your questions.

Mr. MICA. Thank you.

We will hear from our last witness on the panel, Brenda Sprague, Deputy Assistant Secretary for Passport Services with the Department of State.

STATEMENT OF BRENDA SPRAGUE

Ms. SPRAGUE. Mr. Chairman, Ranking Member Connolly, and distinguished members of the subcommittee, thank you for the opportunity to testify today about the Department of State's role in the U.S. ePassport and Passport Card programs.

I think we all agree the integrity of the U.S. passport is essential to our national security and the protection of our traveling citizens. We believe that issuing secure travel documents to qualified citizens is a cornerstone of our national mandate. In pursuit of this mandate, we have spent years creating a physical passport with security features, a photo biometric, and enhanced electronics that render a U.S. passport virtually impossible to counterfeit.

We are proud of this achievement and we are not resting on our laurels. We are well into the planning and development process for the next generation passport.

Having a high quality physical document is not enough. It is only in conjunction with our highly trained passport adjudicators and fraud prevention managers that access to the document remains secure.

Their attention to detail, specialized knowledge, and daily commitment to excellence are central to our ongoing efforts to ensure that only qualified U.S. citizens ever get the opportunity to have and use a U.S. passport.

Passport adjudicators spend hours annually in mandated training to make certain their skills are up to this monumental task. We conduct systematic audits of our issuance to identify errors in adjudication. We have also built anti-fraud tools into the adjudication process to assist them in this endeavor.

Passports are issued based on a review of citizenship and identity documents issued by Federal, State, and local jurisdictions. Our ability to verify the accuracy and authenticity of those documents is greatly enhanced by real-time information sharing and cooperation with the issuing agencies.

In the last six months, we have incorporated the FBIs NCIC Supervised Release files and a real time Social Security check into our front-end verification process. Additionally, we use the National Law Enforcement Telecommunications System's network to verify driver's licenses. We are working with State vital record bureaus to encourage participation in a national centralized database of birth and death records.

We believe data-sharing programs like these are essential tools for verifying the identity and entitlement of passport applicants, and we continue to pursue opportunities to expand these efforts among Federal, State, and local agencies.

Biometrics provide for an additional level of security to ensure that these documents are not fraudulently altered or used. Using facial recognition, all photos submitted by passport applicants worldwide are screened against the State Department's extensive database of facial images to confirm identity, as well as to detect fraudulent applications.

Since 2006, the ePassport has been in the vanguard of our effort to improve border security. It is fully compliant with the recommended specifications for machine-readable travel documents of the International Civil Aviation Organization, ICAO. It has printed biographical data protected with secure laminate and many other security features to protect the integrity of the document and deter counterfeiting.

The passport also contains an integrated circuit or chip. The personal data stored on the chip is identical to the data that is printed visually on the data page, including a digital photo image of the passport bearer. A unique signature is written to the chip, completing what we call the Public Key Infrastructure, PKI, process. The chip is then locked so the data can never be changed. The Department believes that the various security features, combined with the use of PKI, mitigates the risks associated with altering data from the book or chip.

In July 2008, the Department of State began issuing passport cards which incorporate vicinity read RFID technology. These cards are designed to facilitate the frequent travel of U.S. citizens living in border communities. With this technology, CBP inspectors at U.S. land and seaports of entry are able to verify the traveler's identity before the traveler reaches the inspection station. The card has forensic security features to guard against tampering and counterfeiting, and to give CBP officers see and feel cues to verify the card.

To have the world's most secure travel documents requires that we continually assess the security features and design of the passport and passport card for potential vulnerabilities and risks, and to incorporate new measures as technology advances.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.

[Prepared statement of Ms. Sprague follows:]

DEPARTMENT OF STATE

STATEMENT

OF

BRENDA S. SPRAGUE

DEPUTY ASSISTANT SECRETARY FOR PASSPORT SERVICES

BEFORE THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITTEE ON GOVERNMENT OPERATIONS

HEARING

ON

GOVERNMENT ISSUED IDENTIFICATION CARDS

WEDNESDAY, June 19, 2013

Thank you for the opportunity to testify today about the Department of State's role in the U.S. ePassport and Passport Card programs.

I think we all agree: The integrity of the U.S. passport is essential to our national security and the protection of our traveling citizens. By U.S. Passport, I am referring to both the Passport Book and Passport Card. At the Department of State, we believe that issuing secure travel documents to qualified citizens is a cornerstone of our national mandate. In pursuit of this, we've spent years creating a physical passport with security features, a photo biometric, and enhanced electronics that render a U.S. ePassport virtually impossible to counterfeit.

We are proud of this achievement, but we are not resting on our laurels. We are well into the planning and development process for the next generation passport. We have gathered an elite team of experts on document security and design and border control systems from across the Bureaus of Consular Affairs and Diplomatic Security, the Department of Homeland Security's (DHS) Customs and Border Protection (CBP) and Immigration and Customs Enforcement, the Bureau of Engraving and Printing, and the Government Printing Office's (GPO) Security and Intelligent Documents office to serve on the Next Generation Passport Working Group.

The Group is charged with evaluating passport design concepts and new technologies and developing recommendations based on their relative impact and advantages. The group is looking at the possible use of laser engraving on a plastic bio-page which would allow the Department of State to leverage the enhanced security found in the Passport Card for the passport book. Also, we are looking at laser perforating the pages of the passport to help combat page substitution, a feature commonly found in the passports of other countries.

The Department plans to deploy the next generation passport in 2015. This timeline includes extensive testing of the durability of the new passport and its ability to withstand alteration and counterfeiting attempts. These tests are conducted with industry experts in the areas of product durability, operations, and adversarial analysis within the government and in the private sector.

The Department of State prefers for the components of the passport book, particularly the chip, to be "Made in America" as much as possible. GPO, which manages the contractual relationship with vendors that supply the materials for the passport book, has successfully engaged suppliers and now almost all components and raw materials for the passport book are made in the United States.

Having a high-quality physical document is not enough. It is only in conjunction with our highly-trained passport adjudicators and fraud prevention managers that access to the document remains secure.

The dedication and expertise of these employees not only helps protect our borders, it also helps drive our economic engine – ensuring U.S. citizens can travel for work, for pleasure, and to visit family and friends abroad.

Passport adjudicators spend hours annually in mandated training to make certain their skills are up to this demanding task. We've also built anti-fraud tools into the adjudication process to assist them in this endeavor.

Passports are issued based on review of citizenship and identity documents issued by federal, state, and local jurisdictions. Our ability to verify the accuracy and authenticity of those documents is greatly enhanced by real-time information sharing and cooperation with the issuing agencies.

In the last six months, we have incorporated the FBI's National Criminal Information Center NCIC Supervised Release files and a real time Social Security check into our front-end verification process. Additionally, we use the National Law Enforcement Telecommunications System network to verify driver's licenses. We are working with state vital records bureaus to encourage participation in a national centralized database of birth and death records provided by The National Association for Public Health Statistics and Information Systems. We also use the services of several commercial data providers which allow our employees to verify an applicant's social footprint and detect fraudulent addresses, phone numbers, and other discrepancies in an applicant's data.

We believe data-sharing programs like these are essential tools for verifying the identity and entitlement of passport applicants, and we continue to pursue opportunities to expand these efforts further among federal, state, and local agencies.

Since August 2006, the ePassport has been in the vanguard of the effort to improve border security. It is fully compliant with the recommended specifications for machine-readable travel documents of the International Civil Aviation Organization (ICAO). It has printed biographical data protected with a secure laminate and many other security features to protect the integrity of the document and deter counterfeiting, including micro-printing, color-shifting optically variable security ink, and random florescent fibers. The passport also contains an integrated circuit or chip. The personal data stored on the chip is identical to the data that is printed visually on the data page along with a digital photo image of the passport bearer.

The Department's Travel Document Issuance System (TDIS) resides on a secure State intranet. It uses data from the individual's application to create a unique, one time signature and sends that back to TDIS. That unique signature is then written to the chip, completing what we call the Public Key Infrastructure (PKI) process. The chip is then locked so that the chip can't be written to again and to prevent the data on the chip from ever being changed.

To prevent skimming and eavesdropping of data, Basic Access Control (BAC) is employed. BAC is similar to a PIN used in ATM or credit card transactions. In the case of the electronic passport, characters from the printed machine-readable zone of the passport must be read first in order to unlock the chip for reading. Thus, when an electronic passport is presented to an inspector, the inspector must scan the printed lines of data (MRZ or Machine Readable Zone) in order to be able to read the highly protected data on the chip. To further protect against skimming, the U.S. passport also includes a shielding material in the passport cover that complicates attempts at skimming as long as the passport is closed.

Finally, in order to mitigate the ability to track individuals, the chips used in U.S. electronic passports have randomized Unique Identifiers – or UIDs. Randomized UIDs allow the U.S. passport to change its chip identifier each time it is powered up, thus preventing tracking via that number. The Department believes that the use of PKI, BAC, shielding material, and randomized UIDs mitigates the risks associated with skimming or altering data from the chip. It is highly unlikely that U.S. ePassports could be altered in any way while they are being held by a foreign inspection authority or hotel. The U.S. ePassport protects the privacy of all U.S. ePassport bearers from nefarious acts.

Biometrics provide for an added level of security to ensure that these documents are not fraudulently altered or used. Using Facial Recognition (FR), all photos submitted by passport applicants worldwide are screened against the State Department's extensive database of facial images to confirm identity as well as to detect fraudulent applications. To improve the effectiveness of our FR system, we have worked to improve the quality of the passport photo by updating our software and implementing a printer calibration standard which allows for the printing of clearer images. We have also designed a brochure showing acceptable and non-acceptable photos which is being distributed to our more than 8,000 passport application acceptance facilities across the country.

In July 2008, the Department of State began issuing passport cards enhanced with Radio Frequency Identification (RFID) technology to allow for U.S. citizens to reenter the country via land or sea from Canada, Mexico, Bermuda, and the Caribbean as part of the Western Hemisphere Travel Initiative. The Department of State designed the new Passport Card to be as tamper and counterfeit-resistant as possible. The card has forensic security features to guard against tampering and counterfeiting and to give -CBP officers "see and feel" cues to verify the card.

We also work with CBP to evaluate the use of the RFID technology at the borders to ensure the Passport Card meets their operational needs. In previous versions of the passport card, we encountered an unacceptable read-rate. The Department instituted additional RFID testing prior to use at our personalization centers to ensure we were providing the public with the best possible product. With the release of the updated Version 3 Passport Card in summer 2012, which included improved RFID technology, and CBP's improved reader software, we have virtually eliminated what State and CBP both considered a challenging problem.

The most obvious security feature of the passport card is the use of laser engraving which is extremely difficult to forge or counterfeit, in place of standard photo dye sublimation images used in standard identity cards. The Department is also using an optical variable device (OVD), similar to a hologram, embedded inside the card. The embedded OVD overlaps the laser-etched photograph below the card surface. Any attempt to alter the OVD or the bearer's image will destroy the integrity of the card.

To facilitate the frequent travel of U.S. citizens living in border communities and to meet DHS's operational needs at land borders, the passport card incorporates vicinity-read RFID technology. With this technology, Customs and Border Protection inspectors at U.S. land and sea ports of entry are able to verify the traveler's identity before the traveler reaches the inspection station. To protect the privacy of citizens, a protective sleeve is provided with each passport card to guard against unauthorized reading or tracking of the card when it is not in use.

We have made a few notable upgrades to the security of the passport card since its introduction in 2008. In April 2010, we introduced a secondary "Ghost" image of the bearer formed by repeated lines of text. This text, generated by a security algorithm, varies according to the bearer's personal data. In December 2012, we introduced a new composite card made almost entirely of polycarbonate. The manufacturing process of this new card fuses each layer so that it makes layer separation extremely difficult.

Before releasing a new version of the passport card, we require many different testing protocols. As the card is valid for 10 years, we conduct rigorous durability tests at different stages of card manufacturing. The Department works with CBP to conduct operational testing to evaluate how the RFID chip responds to their equipment at the borders. We also work with the DHS' Homeland Security Investigations Forensic Laboratory to leverage their experiences with similar documents issued by foreign nations to evaluate the security features, construction, and personalization of the card for their opinion from a counterfeit deterrence perspective.

This multi-step approach to testing all of our documents has proven to be effective; to have the world's most secure travel documents requires that we continually assess the security features and design of the passport and passport card for potential vulnerabilities and risks and incorporate new measures as technology advances.

Thank you again for the opportunity to appear before you today. I am happy to answer any questions you may have.

Mr. MICA. Well, I thank the witnesses for their testimony and now we will turn to questions.

First, Mr. Romine, welcome. I am sorry to see that your predecessor has retired, who testified back in April several years ago, what was it, 2011, that it would just be a matter of months. You heard that testimony. How do you respond to her testimony? And we swore her in, too. I think I did. Maybe I didn't; maybe that was the problem. Ms. Furlani said, oh, yes. Not one yes, but two yeses, that they would have that standard for biometric iris.

Mr. ROMINE. Yes, sir. So thank you for the question. I know Ms. Furlani very well and I can guarantee she had no intent to deceive the subcommittee.

Mr. MICA. But that was April 14th, 2011.

Mr. Connolly, is today 2013? Is this June? What is the date?

Mr. CONNOLLY. June 19th.

Mr. MICA. June 19th.

What has happened?

Mr. ROMINE. Thank you for asking.

Mr. MICA. Your worst nightmare has come true, I am back and chairing a committee with broad jurisdiction.

Mr. ROMINE. What I can tell you is that——

Mr. MICA. How long? What are you going to tell us? Where is the iris standard?

Mr. ROMINE. Well, if I can expand a little bit first on the testimony of Ms. Furlani. It was predicated, as she stated at the time, on the assumption that no major technical hurdles would surface.

Mr. MICA. My God, technical hurdles? We asked for this after 2001, and they were working on it. This is to 2011. We were promised it was, I mean, at least three times in three different appearances, it was just around the corner. This is 2013. When? When, when, when can we get—I don't want to harass the witness. Sir, please tell me when we can get this standard. These people can't do a damned thing unless you set the standard. That is what they are going to testify to when I go after them in a minute.

Mr. ROMINE. During the public comment there were three major technical issues.

Mr. MICA. Tell me the when. Is it an estimate? A month? A week? Two more years? When can you set a standard?

Mr. ROMINE. We expect to be able to release the special publication immediately after the workshop that we are holding in early July. So on July 9th we will hold a workshop on a camera certification, iris camera certification. Our expectation is that we will be able to release the second edition or the second version of Special Publication 876 at that time, or immediately thereafter.

Mr. MICA. So say by September 1st these agencies should have some standard to go by?

Mr. ROMINE. At the risk of repeating the mistake of a predecessor in your view, I would say I am willing to agree that that is an appropriate release time.

Mr. MICA. Mr. Connolly, if I die or you guys take over, do you pledge to follow up on this?

Mr. CONNOLLY. We don't want you to die, Mr. Chairman, but we certainly want to take over, and I do make that pledge.

[Laughter.]

Mr. MICA. Okay.

Mr. ROMINE. We certainly want to be responsive to the subcommittee's concerns.

Mr. MICA. Well, again, you just heard testimony. They are producing documents to which we don't have dual biometrics. The Canadians have had a system, I went to see it, since 2007; it has both. I told Mr. Connolly I went to Amsterdam; I saw they put the fingerprints, the iris, and they went through the turnstile. But it is the only way you can absolutely confirm the identity of that individual, according to the technology that is available today. Is that pretty much correct?

Mr. ROMINE. I would not say that necessarily.

Mr. MICA. But, again, unless we have some check.

Now, Mr. Martinez, with the FBI, you do fingerprints. Fingerprints can be tampered, can they not, sir?

Mr. MARTINEZ. Yes. There are several examples of people who have attempted to obscure surgically alter their fingerprints.

Mr. MICA. Okay. So we are finished with you, Mr. Martinez. You can go. No, just stay.

But, again, our best bet, we were told this after 2001, was to have iris and fingerprint.

Mr. Allen, welcome. FAA. And we are still producing the Wilbur and Orville Wright. You saw they are dead; I confirmed it. And now you come before me and you testify. I just about went out of the seat and over the podium to get you, restraining myself, did not contemplate the use. We put it in law that you would have a durable biometric with a photo of the pilot. Never said anything about Wilbur and Orville. I never put it in any law; it wasn't in the most recent 2012 law.

But you did not contemplate. Then you came before us today and used the excuse of the law that redirected you to do what we told you in the beginning as an excuse for not performing. Is that right?

Mr. ALLEN. Yes, Mr. Chairman.

Mr. MICA. Oh, my God.

Mr. CONNOLLY. Mr. Chairman, could I just clarify what I just heard?

Mr. MICA. Yes.

Mr. CONNOLLY. Mr. Allen, did you just testify under oath confirming what the chairman asserted, that you used the law to not comply?

Mr. MICA. He is using it as an excuse.

Mr. CONNOLLY. But that was his question.

Mr. MICA. We put it in the law because they hadn't done it in the beginning, and he says, well, and then he says we never contemplated that this could be used for an ID. What the hell were they going to use it for?

Mr. CONNOLLY. I know.

Mr. MICA. You used it to get into the Regal theaters on Friday night with a senior discount?

Mr. CONNOLLY. Mr. Allen, I just wanted to make sure I understood what you said because that is what you said, and I want to give you the chance to either expand or clarify.

Mr. ALLEN. Thank you, Mr. Connolly. What I testified to was that we already had a rulemaking process in place that was meeting specific issues from that rulemaking and we received another legislative requirement, and some aspects of that were not identified in the earlier legislation.

So when you get into rulemaking and you got that thing going in process and you are addressing those issues, it wasn't addressing some of the things that were brought up in the second legislation. That is what I was saying.

For instance, iris scan. The iris scan was not in the first one; it is in the second one. So, consequently, the iris scan was not entertained, was not being addressed in the first rulemaking process, so now we have iris scan we have to address.

Mr. MICA. I am taking back my time.

Biometric would include fingerprint and iris. That was in the original law. Where is the original law? Doesn't the original law that I passed say that, in fact, you would have to have biometric capability?

Mr. ALLEN. Yes, sir, it says accommodating a digital photograph, a biometric identifier. And there is some debate as to whether it has to be an iris scan or it can be a fingerprint or something like that. So, therefore, that first rulemaking was not entertaining the iris scan.

Mr. MICA. And then you suddenly said you couldn't contemplate it being used for security. Again, what were they going to do with it?

Mr. ALLEN. Sir, as you know, and as my boss testified earlier, this was originally for a license.

Mr. MICA. Well, again, I don't know how we could make it any clearer that we are trying to get a pilot, and you don't have to put the photograph on it, it could be embedded in it. You would be better off telling me some standards hadn't been set for that as an excuse.

But I am telling you this is highly frustrating, and I expect, and we will haul you back in here, that we get a pilot's license that meets the intent of the law, that can be used, so a pilot who is going to the airport to get on a plane to fly a commercial passenger aircraft, we know who that individual is and we have some certainty of it, okay? We have been lucky so far. And now they have a known pilot program. If they get any more lanes at the airport of programs, there won't be room for the passengers. We have, at least one airport, probably a dozen different lanes now.

Ms. Manaher, I just described the Global Entry experience. I don't mean to get personal in these hearings, but I had to relay my wife's experience of not qualifying for pre-check, so she goes to Global Entry, and then you produce a card the way the form is set up that requests her name, and she ends up with her maiden name on her passport, Ms. Sprague's passport, and her middle name on the Global Entry card. Is she going to be accepted by Sprague now?

Ms. MANAHER. [Remarks made off microphone.]

Mr. MICA. Yes? Even though it doesn't match? Had anyone given any thought to having the requirement even in the form that the passport match the Global Entry?

Ms. SPRAGUE. Colleen, it is your form.

Ms. MANAHER. Sir, it is my understanding that is now fixed for Mrs. Mica.

Mr. MICA. Oh, I don't care about Mrs. Mica.

Ms. MANAHER. Oh, oh.

Mr. MICA. Don't tell her I said that.

[Laughter.]

Mr. MICA. I am just talking in general.

Mr. CONNOLLY. I move that be stricken from the record.

[Laughter.]

Mr. MICA. Without objection, that is stricken from the record.

I am talking about, again, it is a simple thing that your form should, if you are producing all of these Global Entry documents, that they should match the passport. Basic? Can we look at that?

Ms. MANAHER. Yes, of course, sir.

Mr. MICA. At least look at the form or something. And you are very nice people and you are here, but when you get to that agent that is responsible for checking the documents and they don't match, I have seen people in tears at TSA lines because their ticket doesn't match their ID exactly.

Have you given any contemplation to incorporating an iris in the future, in addition to a fingerprint, on your documents?

Ms. MANAHER. Yes, sir. As you know, our NEXUS program with Canada we do use an iris, and I do believe that both iris and facial recognition——

Mr. MICA. What standard are you using on the NEXUS for the iris?

Ms. MANAHER. It is the Canadian standard, sir.

Mr. MICA. Yay. How about if we put in law that we just adopt the Canadian standard? They have had it since 2007. Have you ever known an instance in which it has been thwarted?

Ms. MANAHER. Not to my knowledge, sir.

Mr. MICA. So others have done this.

Is anyone familiar with the CLEAR program? We couldn't get CLEAR to testify; they are terrified, and I don't blame them, to come before a panel and actually tell us they have something that works. Probably they would be stricken from the Federal qualified vendor list.

Mr. Connolly, I will let you go at it a little while.

Mr. CONNOLLY. Thank you, Mr. Chairman.

I think the frustration being expressed here is that it has now been 12 years since the tragedy of 9/11 and we seem not to have resolved this problem. We don't have a uniform standard; we haven't agreed on whether the appropriate biometric standards. We have spent a lot of money on an ID card that doesn't work very well, even though there are examples within the United States Government of ID cards that do work.

And even listening to all of you, if you flew in here from some other place and didn't really know much about the subject, it sounds a lot like stovepipe; well, I don't know what anyone else is doing, but here is what the FBI is doing.

Ms. Manaher and Ms. Sprague, if there is a program that ought to be cross-fertilized, it is Global Entry and the passport. And yet I think they were developed separately. Is that correct?

Ms. MANAHER. We have a very close partnership with Department of State, but, yes, they were developed separately. But we used a similar international standard, sir.

Mr. CONNOLLY. And, Ms. Sprague, what is the rationale for developing these programs separately?

Ms. SPRAGUE. The passport has a different purpose than Global Entry. But I would note that your passport is the token you use to activate Global Entry when you enter the United States, so we are sharing that technology and that is the way it works. But the Global Entry card is also used for TSA pre-check.

Mr. CONNOLLY. I understand. But understanding the overlap, when they were developed, did these two agencies cooperate in the development of the technology and in the statement of needs, in the RFP or whatever it was?

Ms. SPRAGUE. I don't know how formal the process was, but I know in anything we do with the passport we invite Customs and Border Protection, as well as ICE and the Government Printing Office and others are involved in the development of all our standards so that they all work. Our passports have to work with what CBP is doing at the borders, so that is a constant interchange daily that we are communicating on those standards and the interoperability of our documents with their systems.

Mr. CONNOLLY. Mr. Allen, you testified that the FAA hadn't foreseen the use of iris as a biometric index or standard. Why not? I mean, isn't this more than what the Congress explicitly spells out? Isn't this somewhat what the FAA thinks we need to protect the Country, and did that never come up and was it rejected? Why wasn't that included?

Mr. ALLEN. Good question, Mr. Connolly. No, it wasn't rejected outright, it just was not mature at the time, to meet the requirement.

Mr. CONNOLLY. I am sorry. You mean the technology was not?

Mr. ALLEN. Well, the iris scan technology and standards were mature at the time, but this was back in 2004 for that initial legislation, so we were looking at biometrics of the proven fingerprints, a picture, and going down that path, and then when we got this next legislation that suggested, or actually required, iris scanning. Now we have to change course and also find out what that standard is, and to accommodate that extra biometric into a proposed license or a proposed certificate.

Mr. CONNOLLY. The chairman pointed out that the picture on a pilot's license is that of Orville and Wilbur Wright. To vote these days I need to produce a driver's license with my picture on it. Not a very good picture in Virginia, I might add, but that is a different matter. But why wouldn't we have airline pilots' pictures on their own ID, rather than Orville and Wilbur Wright?

Mr. ALLEN. We will get there. We intend to fully get there, but we want to make sure that you don't come back and complain about our program like you are complaining about the TWIC program. There is a foundation we have to set in here and there is a system behind this that we have to do smartly so that we don't put or exercise an undue economic burden on pilots and we do it smartly. We are learning a lot from the Global Entry program, and as of today they do have to submit a picture ID with their pilot's license, so there is actual verification—I have a Virginia driver's license as well—that picture, that they have——

Mr. CONNOLLY. Did they make you take your glasses off?

Mr. ALLEN. Yes, sir, they did.

Mr. CONNOLLY. And you couldn't smile?

Mr. ALLEN. No, I couldn't.

Mr. CONNOLLY. Yes, I know.

Mr. ALLEN. So you do have that security right now. So we believe we are going at it smartly and we are working with TSA so we don't have stovepipe, as you suggested earlier, so that we don't go out shooting from the hip and doing undue harm on the public by requiring something that is not in concert with other Government agencies, so we have some standardization.

I share your frustration as well. I have more cards, including a military ID card. I understand what you are saying. We understand the intent and we intend to meet that, but we have to establish a good foundation now and set the system behind it so that we don't have the public incur a financial liability that they will push back on.

Mr. CONNOLLY. Those are all good points. I think, however, you might concede that I think to the public it will come as a surprise to learn, 12 years after 9/11, we still don't really have a photo ID requirement for the license itself. I think that is somewhat shocking to the public.

Mr. ALLEN. Yes, sir, I would agree that that would look shocking.

Mr. CONNOLLY. All your points notwithstanding, because I think we do want to get it right. But it has been 12 years. When are we going to get it right?

Mr. ALLEN. Well, when we do the whole megillah. I mean, just put a picture on there is one thing, but to put the picture and biometrics and also to work with other Government agencies to make sure we are congruent with them, to also work with the public and the airlines and the pilots to help them understand what the systems are. And we are not even talking about the infrastructure out there that would be needed to put in place for regulating access to secure areas of the airport. There has to be due diligence.

Mr. CONNOLLY. Well, let me ask you this, Mr. Allen. Even before we get to the biometrics, your point is let's do it all at once, and that is a good point. But if I purport to be a pilot or if I am a pilot, as I am going through the system, am I ever required, actually to get on the airplane, to show somebody a photo ID?

Mr. ALLEN. Yes, sir, you are. You are required to do that.

Mr. CONNOLLY. All right. So it is not like we are totally ignoring that.

Mr. ALLEN. No, sir.

Mr. CONNOLLY. The fact that it is not on the pilot's license, per se, doesn't mean there isn't some sifting and sorting in terms of verification and validation.

Mr. ALLEN. Yes.

Mr. CONNOLLY. All right.

Mr. Romine, NIST is charged with trying to set a standard so we do avoid the stovepipe Mr. Allen and I were just talking about. Again, what one does not sense is that we, as a unified Government, are seized with a mission here. Now, absent some kind of effective biometric ID standard, you ask yourself what could go wrong with that, the absence of that. And we all know; we can all speculate on the answers to that.

Frankly, Ms. Furlani, maybe she meant well, maybe she believed what she said. I am sure she did. But now she is not accountable. So it is easy to reassure Congress and the public, through its Congress, when you are on the brink of retirement and you won't be the one testifying next time, poor Chuck is. And I don't mean to suggest she did that deliberately, but I will say to you it is a little troubling.

I mean, where does that end if everybody who comes here and testifies on behalf of a Federal agency is watching the clock in terms of I retire in two months, so I won't have to be back here and explain myself. But why, two years later, two years and two months later, actually what I gave assurances for did not happen and we are not even within sight of it happening? So I think that is the frustration you are hearing.

But are we seized with a mission? And how can we provide guidance to Federal agencies, including your colleagues at this table, through a robust, rigorous process and standard setting by NIST on something so vital?

Mr. ROMINE. So you have keyed on exactly the right point. First of all, I am happy to be accountable for this to this subcommittee. I have told my staff I only have another 23 years in this job. I have done two; 25 is my limit.

Mr. CONNOLLY. You are not going to retire on us?

Mr. ROMINE. I will not retire anytime soon.

Mr. MICA. They are only in the second decade; we can get him into the third.

[Laughter.]

Mr. ROMINE. But you have hit on it, which is this robust process that NIST manages that is a process whereby we convene the best technical experts, nationally and internationally. And during that process in the iris case we received many comments, but several of them were sufficiently of concern to us that we feared that, unless we resolved them, it would derail our ability to stand behind the iris standard, and those three are the compression of the iris image and the size of the resulting image, there were constraints on it, on how large it could be. We wanted to be sure that that would still give us sufficient comparability.

The second, the community had expressed some concern about iris changes with age, and to avoid the potential of frequent re-enrollment because of iris changes as people age, we wanted to do the research necessary before we issued the guidelines.

And then the third was the camera certification that I alluded to earlier, and not putting the Government in a position of having vendors come in with claims about camera capabilities that weren't backed up.

Those three things were of sufficient concern to us that we have spent now, as you point out, a significant fraction of our time resolving those issues. So we have been very active in this space and I am pleased to report that in each case we have had successful resolution. We have determined that the compression level that we are required to adhere to for interoperability with some of the identity cards that Federal agencies are using is not an impediment.

We have done extensive research on a very large collection of iris images that date as long as a decade with the same individuals' images over a 10-year period, and we have determined that change due to aging in iris is not an impediment. That is a recent finding from our researchers. And we have now put in place all of the tools that we need for certification of the quality of iris cameras.

Mr. CONNOLLY. Mr. Chairman, you have been most indulgent. Just two more questions, if I may.

Mr. MICA. No, go right ahead.

Mr. CONNOLLY. I assume part of the process is you are looking at best practices, you are benchmarking with other entities, other countries.

Mr. ROMINE. That is correct.

Mr. CONNOLLY. The chairman, for example, mentioned Amsterdam, so presumably you have looked at what they do.

Mr. ROMINE. We engage with the international community broadly through the standards development process, yes.

Mr. CONNOLLY. But hopefully we are going to adopt best practices if we think they are best practices.

Mr. ROMINE. Absolutely.

Mr. CONNOLLY. For example, Ms. Manaher's organization has already adopted the Canadian best practices because they work. Is that correct?

Mr. ROMINE. I believe that that decision was made as a result of the fact that they wanted to move forward. Our concern is we have to do the absolute best standards development and coordination that we can do on behalf of the Federal Government in the United States.

Mr. CONNOLLY. I understand. But if you were to look at best practices and discover, I don't know, the Cote d'Ivoire standards are the best in the world and there is just no beating that based on everything we know, why not adopt it?

Mr. ROMINE. That is our standards development process.

Mr. CONNOLLY. Okay.

Mr. ROMINE. We engage the international communities.

Mr. CONNOLLY. And the second question is and does NIST look at what we are doing at Federal agencies to avoid the stovepiping, to avoid the duplication of effort and to make sure that in fact we are coordinating so that, for example, where Global Entry leaves off the passport begins, or vice versa, so that we are not creating two separate systems that don't really synchronize?

Mr. ROMINE. Yes, in the sense that NIST, by statute and by administration ruling, is the agency that is charged with coordinating both the development and the adoption of standards. Those standards are generally, again, by statute and administration ruling, we engage the private sector. Most of the standards development activity in the United States, unlike other countries, is led by the private sector, with NIST as the coordinating role on behalf of the Federal Government.

Mr. CONNOLLY. But you are not a policeman. You don't have the authority to tell the State Department you are not going to issue that kind of passport because of X, Y, and Z.

Mr. ROMINE. That is correct.

Mr. CONNOLLY. But can you be a clearinghouse to say—I am just using the State Department as an example—gee, in our research here is something you may want to look at; you don't really want to do that, upon reflection, because here are the problems that have occurred with that and oh, by the way, country X has great experience you may want to look at because that is a standard we are probably going to incorporate?

Mr. ROMINE. We do routinely engage with Federal agencies as part of our role, and agencies have standards officials that are attune to the work that NIST is doing on their behalf and on behalf of the Federal Government.

Mr. CONNOLLY. But you do play that clearinghouse role?

Mr. ROMINE. We do play a role in coordination. Clearinghouse, I am not sure. That conveys a sense in which we are a gatekeeper, and I don't think we can, as you point out, we don't have authority in this case.

Mr. CONNOLLY. Well, I don't mean it as a gatekeeper, I mean it as the compiler of sort of universal information.

Mr. ROMINE. Yes.

Mr. CONNOLLY. The State Department hasn't got the time or resources to look at best practices everywhere.

Mr. ROMINE. Yes.

Mr. CONNOLLY. That is your job.

Mr. ROMINE. That is our role.

Mr. CONNOLLY. Okay.

Mr. Chairman, thank you.

Mr. MICA. Thank you, Mr. Connolly. And if you want to excuse yourself for that, I will finish up.

Well, it is interesting today to hear, first of all, Customs and Border Patrol here actually has implemented the use of iris and the Canadian standard.

Ms. Sprague, did they consult with you when they did that? You say you guys work hand-in-glove?

Ms. SPRAGUE. We were aware that they were moving ahead with that program, but the border is the responsibility of Customs and Border Protection, and if they choose to accept a document or go in another direction, they certainly have the authority to do so.

Mr. MICA. But they did consult with you? You do know they are using that?

Ms. SPRAGUE. Yes, we do.

Mr. MICA. Okay. Does your passport have the ability to incorporate a biometric standard, both fingerprint and iris?

Ms. SPRAGUE. Yes, it does.

Mr. MICA. It does? So when they set the standards, you have the capability and the document could incorporate that?

Ms. SPRAGUE. Yes, it does. But, if I can, the question, the challenge will be the capture of that data. We have 113 million passports that do not have a secondary biometric. We are issuing about 13 million passports a year. We have to find a way to capture that.

Mr. MICA. It would seem that you would start with renewals. Now, when they issue a visa, does that have a biometric capability embedded in the visa document itself?

Ms. SPRAGUE. The visa document, when it is read at the border, it points to the computer, which does have the match to the fingerprint. So we have captured the fingerprint overseas.

Mr. MICA. And that can also be incorporated to include iris in the future?

Ms. SPRAGUE. It can be.

Mr. MICA. Okay. Because, again, if you look at most of the instances where we are trying to identify folks, whether it is issuing a visa from Nigeria or Yemen, or wherever, that we know who is who and we can also track those people.

I did not know, and I asked staff to see if there is any Federal agency. Mr. Martinez, are you aware of any Federal agency or do you have any use of dual biometric iris, either internally, or do you know of any agency that uses it, both fingerprint and iris?

Mr. MARTINEZ. I am not aware in the context of credentialing. We have an iris pilot where we are looking at iris as another identifier or a technology that we can use to add to our identification file with fingerprints and other data.

Mr. MICA. We are told the military does use some; I think they use it for some access, and they have a system they have agreed on. I think it is in Afghanistan, maybe some other post. CIA, we didn't call them in, but I am sure they have some sophisticated credentialing that is available.

Now, Mr. Romine, you had testified that you are getting close, and I am holding you to maybe some time this summer. In previous meetings, when we had your predecessor folks in before, there was a panel or interagency group that met to discuss these. Does that still exist, the standards?

Mr. ROMINE. Under the NSTC, the National Science Technology Council, there was a biometrics and identity management subcommittee, and I believe that is still active. But I can double-check that.

Mr. MICA. That worries me, I believe that is still. Now, if anybody, you should know because Mr. Connolly just talked about stovepiping, and the only way we are not going to stovepipe it is for people to be talking, meeting, discussing. When is the last time the group met? Did you ever meet with them?

Mr. ROMINE. I have not met with them.

Mr. MICA. Are you in charge of setting the standard or overseeing it?

Mr. ROMINE. I manage the laboratory.

Mr. MICA. And have you been at one of these meetings?

Mr. ROMINE. I haven't personally been.

Mr. MICA. Now I am really getting worried. Has anybody here been to any of those meetings? No, Mr. Allen? Mr. Martinez, you are the standards guy with FBI. Have you ever been to a meeting? The interagency meeting where we set down and discuss the credentialing standards.

Mr. MARTINEZ. That would be out of the responsibility of my particular branch. I would probably have to defer to our security division.

Mr. MICA. To see if somebody had been.

Ms. Sprague, anyone? Have you guys been to one lately?

Ms. SPRAGUE. We attend a lot of meetings, but I don't know that we ever attend that specific one.

Mr. MICA. Okay. I guess if I put it in law that they should attend the meetings, that would be used as an excuse because we didn't require that before, and it would set us back further.

How about guys getting together, Mr. Romine?

Mr. ROMINE. I am sorry?

Mr. MICA. Can we see if the subcommittee is activated?

Mr. ROMINE. Of course.

Mr. MICA. Who is in charge of the subcommittee, does anyone know?

Mr. ROMINE. It is managed by the Office of Science and Technology Policy at the White House.

Mr. MICA. Oh, okay. Just like IRS, it leads to the White House. I am just kidding.

[Laughter.]

Mr. CONNOLLY. I move that be stricken from the record again.

Mr. MICA. All right, we will take that one too. We can have a little humor at these meetings.

Well, we have to get people talking to each other. We have to get the standards set. We spent billions. I had the staff starting to count this. TWIC is half a billion by itself. Now, because they don't have a reader, we haven't incorporated a dual biometric, they are talking about just using it as an ID. Pretty expensive ID card for the taxpayers to foot that.

We have 900,000 airport workers, Mr. Allen. No standardization in identification and credentialing. No biometric standard, right?

Canada has had it since 2007. Have you been to Canada, Mr. Allen?

Mr. ALLEN. Yes, sir. I was in Ottawa about a month ago.

Mr. MICA. And did you see what they are doing?

Mr. ALLEN. I didn't go up there for that purpose, to see what they are doing.

Mr. MICA. Well, that is not the question.

Mr. ALLEN. No, I didn't.

Mr. MICA. Can I talk to whatever his name is, and maybe we can get you a trip up there to look at it? You should go see. It is incredible, the credentialing. And they have within the biometric ID, it has various levels of security clearance, so airport workers can get in to certain parts; pilots can access certain things; access to towers is limited within the credentialing. It goes on and on. And it is replicable and, obviously, if our good friends here from Customs and Border Patrol could adopt their iris as a standard, I have never heard of any thwarting of this system.

Do you ever look at other credentialing, Mr. Romine, in other countries or systems?

Mr. ROMINE. We don't look specifically at credentialing so much as we look at the standards.

Mr. MICA. The standards, right.

Mr. ROMINE. Yes.

Mr. MICA. You have never looked at the Canadian?

Mr. ROMINE. I am sure that we have.

Mr. MICA. You have? Okay. And obviously CLEAR, somebody cleared CLEAR, because they are using iris and fingerprint, and they are using it for travelers. No one is familiar with that program? Did they ever come to you on the CLEAR program?

Mr. ROMINE. I am not aware of a direct engagement, but I can follow up.

Mr. MICA. Again, Mr. Connolly said this looks like a lot of stovepiping. But it doesn't appear that the communications are that good on an interagency basis, and we do need to get a standard in place. Any standard, too, would have to be upgradable, wouldn't it, Mr. Romine?

Mr. ROMINE. That is correct.

Mr. MICA. I mean, since we started this thing in 2012, I think it was when it first started, the technology has dramatically changed, so the standard you set now, 2013, pray to God some time this summer, might need to be upgraded periodically.

Mr. ROMINE. That is correct.

Mr. MICA. But I guess the best way is just don't set anything, so then we don't have to worry about it, and everybody goes off in different directions. We spend billions of taxpayer dollars and we leave ourselves at risk with all kinds of credentialing that doesn't really meet the security test.

Mr. Martinez, thanks so much for confirming that the one biometric method that we have can be thwarted, so that makes me feel good too, that the one biometric measure.

Mr. Allen, he testified to Mr. Connolly that we had three requirements. The first one was that the document be durable. Now, they met that one. They had trouble with the next two. They never got to the bio, and then the photo, of course, that is very complicated to get a photo of a pilot either embedded or on the ID. So they are a third of the way there some decade later. Very encouraging.

Any final remarks, Mr. Connolly?

Mr. CONNOLLY. I look forward to the next hearing, Mr. Chairman.

Mr. MICA. I think we will schedule it for this fall, just to make certain that we follow up.

So I want to thank the witnesses for coming. I am hoping we can make some better progress in the next hearing. We will follow up. This is the first time I think we have ever brought at least this many agencies together. We need DHS. We had them in TWIC last time. Maybe we can get them all back and get a report later this fall.

There being no further business before the Subcommittee on Government Operations, this hearing is adjourned.

[Whereupon, at 11:04 a.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

BIOMETRIC IDs FOR PILOTS
AND TRANSPORTATION WORKERS:
DIARY OF FAILURES

(112-26)

HEARING

BEFORE THE

COMMITTEE ON

TRANSPORTATION AND INFRASTRUCTURE

HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 14, 2011

Printed for the use of the
Committee on Transportation and Infrastructure

Available online at: http://www.gpo.gov/fdsys/browse/
committee.action?chamber=house&committee=transportation

[EXCERPT]

Mr. Mica. And just a final question to Ms. Furlani. The biometric standard for iris, that is still in progress. And while we have some readers, we have 1.5 million TWIC cards that have been issued, but we really don't have readers that are being used on a regular basis. Some, I learned, were approved, but they are not being used. So, we have identification card, which has part of the biometrics.

Your--so it is a twofold question, two-part question. When will you finish the iris capability? And then, when would we have a reader that could actually be used and employ both iris, fingerprint, and of course, it would have the photo?

Ms. Furlani. The iris standard will be--the draft publication will be published in the next--very soon, within days.

Mr. Mica. In the next very soon?

[Laughter.]

Ms. Furlani. Well, hopefully before next week.

Mr. Mica. All right.

Ms. Furlani. But it is in progress. And what that is, of course, has been worked with the industry partners who do develop the cameras that collect the iris information. And one reason that the standard will be so readily adopted is because there are many vendors producing those cameras. So they are available, and they will agree with--be able to use the standard.

Mr. Mica. And when would this standard be issued?

Ms. Furlani. In about--well, we put it out for public comment, we review all those comments, and if there are significant changes that come in, then we would put out a second draft. So it is over a period of months, but it is to be----

Mr. Mica. By the end of the year?

Ms. Furlani. Oh, yes, yes.